REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE ET DE l'INNOVATION

UNIVERSITE GASTON BERGER DE SAINT-LOUIS

U.F.R DE SCIENCES APPLIQUEES ET DE TECHNOLOGIE

CENTRE DE FORMATION PROFESSIONNELLE PLURIDISCIPLINAIRE

Mémoire de fin d'études pour l'obtention du

Master Réseaux et Télécommunications (MaRT)

Un nouveau protocole d'authentification inspiré de la blockchain dans l'IoT

Présenté par :

Mame Mariane Ndiaye

Sous la direction de :

Pr. Chérif DIALLO

Jury :

Président :	M. Daouda SANGARÉ
Examinateur :	M. Abdou Karim MBODJI
Examinateur :	M. Mahamadou TRAORE
Encadreur :	M. Chérif DIALLO

Année Académique 2020/2021

REMERCIEMENTS

Louange à ALLAH le Tout Puissant, le Miséricordieux, sans lui rien de tout cela n'aurait pu être

Merci à ALLAH de nous avoir fait bénéficier de sa protection et de nous avoir donné les moyens de suivre cette formation.

Mes vifs remerciements s'adressent à mes parents particulièrement à ma mère, mes frères et sœurs pour leur soutien moral et leurs encouragements.

Mes vifs remerciements à mon encadrant le Professeur Chérif DIALLO pour sa disponibilité et ses conseils.

DEDICACE

Ce travail est le fruit de plusieurs mois de travail dans les domaines de l'IoT et de la blockchain.

La rédaction de ce mémoire m'est si chère qu'il est de mon devoir de le dédier à :

- Ma mère Mame Diara GAYE, qui peut être fière de trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit. Merci pour les valeurs nobles, l'éducation et le soutien permanent venus de toi.

- Mon père Rawane NDIAYE, mes frères et sœurs Khalilou NDIAYE, Penda NDIAYE et Soukeyna NDIAYE pour avoir contribué à la réussite de ce travail d'une manière indirecte d'y avoir apporté tant d'humeur et d'amour et pour tout le soutien moral prodigué dans les moments les plus difficiles.

- A mes proches, amis et tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

En mémoire Sokhna Soukeyna MBACKE, Birahim GUEYE GAYE, Ibrahima MOLDIO NDIAYE et de Seynabou WADE.

Table des figures

Figure 1: Nabaztag le lapin connecté [6] 5
Figure 2: Domaines d'application de L'IdO [14]. 9
Figure 3: Ecosystème de l'Internet des Objets [15]. 10
Figure 4: Architecture à 3 couches de l'Internet des Objets [18] 15
Figure 5: Architecture à 4 couches de l'IoT [19] 16
Figure 6: Architecture à 5 couches de l'IoT 17
Figure 7: Protocoles réseau IoT mappés sur TCP/IP [21] 20
Figure 8: Les différents défis de l'IoT 22
Figure 9: Taxonomie des schémas d'authentification IoT [25] 30
Figure 10: Structure d'une blockchain 39
Figure 11: Fonctionnement de la blockchain [32] 41
Figure 12: Domaine d'application de la blockchain 47
Figure 13: Architecture du protocole d'authentification pour l'IdO utilisant la blockchain et le fog computing [40] 51
Figure 14: Structure d'un ticket dans Bubbles of trust [37] 55
Figure 15: phase d'initialisations dans Bubbles of trust [37] 55
Figure 16: Phase de création de bulles de confiance [37] 56
Figure 17: Demande d'association [37] 57
Figure 18: Authentification d'un suiveur dans la blockchain [37] 58
Figure 19:Serveur pour la gestion et la distribution de blocs de secrets 61
Figure 20:Structure d'un bloc secret 62
Figure 21:Schéma de la phase d'initialisation du réseau 63
Figure 22: Distribution de blocs de secrets aux différents nœuds IoT 64
Figure 23: Exemple d'attribution de blocs de secrets à des nœuds IoT différents 65
Figure 24:demande de clés publiques aux noeuds voisins 66
Figure 25:Demande d'authentification auprès des voisins 67
Figure 26:Demande d'authentification auprès d'un voisin 67
Figure 27: Vérification des blocs en commun 68
Figure 28:Schéma d'authentification de la version légère du protocole 69
Figure 29:Schéma d'authentification de la version lourde du protocole 69
Figure 30:Relais de message aux autres voisins 70

Liste des Tableaux

Tableau 1: Tableau comparatif de méthodes d'authentification 49
Tableau 2: Tableau comparatif des méthodes d'authentification par rapport à des attaques. 50
Tableau 3:Paramètres du protocole 71
Tableau 4:Analyse du protocole par rapport è la taxonomie de schéma d'authentification 72
Tableau 5:Analyse par rapport aux exigences d'authentification 72
Tableau 6:Résistance du protocole proposé par rapport aux attaques 73
Tableau 7:Analyse du protocole par rapport à certains critères de sécurité 76

Sigles et abréviations

BFT : Byzantine Fault Tolerance

BLE: Bluetooth Low Energy

CoAP: Constrained Application Protocol

DDoS: Distributed Denial of Service

DLT: Distributed Ledger Technology

DoS: Denial of Service

DPoS: Delegated Proof of Stake

ECC: Elliptic curve cryptography

ECDSA : Elliptic Curve Digital Signature Algorithm

ETH: Ether

EVM: Ethereum Virtual Machine

GSM: Global System for mobile

IdO: Internet des Objets

HTTP: HyperText Transfert Protocol

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IoT: Internet of Things

IP: Internet Protocol

LAN: Local Area Network

MAC: Media Access Control

MD5: Message Digest 5

MQTT: Message Queue Telemetry Transport

M2M: Machine à Machine

NFC: Near Field Communication

OWAPS: Open Web Application Security Project

PBFT: Practical Byzantine Fault Tolerance

PoS: Proof of Stake

PoW: Proof of Work

P2P: Peer to Peer

RFID: Radio Frequency Identification

TCP: Transmission Control Protocol

TPM : Trusted Platform Module

UDP : User Datagram Protocol

UIT : Union Internationale des Télécommunications.

WAN: Wide Area Network

WPAN: Wireless Personal Area Network

W3C: World Wide Web Consortium

Table des matières

Table des figures III
Liste des Tableaux IV
Sigles et abréviations V
Introduction Générale 1
Chapitre I : Internet d'objets 3
1.1 Introduction 3
1.2 Définition 3
1.3 Historique et évolution de l'internet des objets 4
1.4 Domaines d'application 5
1.5 Architecture et écosystème 9
1.5.1 Écosystème IoT 9
1.5.2 Architecture 14
1.6 Protocoles 17
1.7 Défis de l'IoT 20
1.8 Conclusion 22
Chapitre 2 : Les aspects généraux de la sécurité dans l'IoT 23
2.1 Introduction 23
2.2 Les services de sécurité 23
2.3 Les vulnérabilités de l'internet des objets 25
2.4 Attaques de sécurité 26
2.5 Conclusion 28
Chapitre 3 : Authentification dans l'IoT 29
3.1 Introduction 29
3.2 Taxonomie des schémas d'authentification IoT 30
3.3 Exigences sur les schémas d'authentification dans l'IoT 34
3.4 Les défis des schémas d'authentification dans l'IoT 34
3.5 Conclusion 35
Chapitre 4 : Blockchain 36
4.1 Introduction 36
4.2 Définition 36
4.3 Origine 36
4.4 Caractéristiques de la blockchain 37
4.5 Structure d'une blockchain 38
4.6 Fonctionnement du réseau 40

4.7 Mécanismes ou algorithmes de consensus 41
4.8 Plateformes Blockchain 43
4.9 Types de Blockchain 44
4.10 Domaines d'application 44
4.11 Conclusion 47
Chapitre 5 : Méthodes d'authentification basées sur la blockchain dans l'IoT 48
5.1 Introduction 48
5.2 Comparaison de différents Méthodes d'authentification 48
5.3 Études de méthodes d'authentification basées sur la blockchain pour l'IoT 51
5.3.1 Protocole d'authentification pour l'IdO 51
5.3.2 Mécanisme d'authentification Bubbles of Trust 53
5.4 Conclusion 58
Chapitre 6 : Proposition d'un nouveau protocole d'authentification inspirée de la blockchain dans l'IoT. 59
6.1 Introduction 59
6.2 Approche : 59
6.3 Schéma : 60
6.4 Phase d'initialisation 62
6.5 Phase d'authentification 65
6.6 Phase de maintenance 71
6.7 Analyses du nouveau protocole proposé 72
6.8 Conclusion 76
Conclusion Générale 77
REFERENCES 79

Introduction Générale

En deux décennies à peine, Internet a profondément changé nos sociétés et nos économies. Il est passé d'une simple technique d'interconnexion des ressources informatiques des centres de recherche travaillant pour le département de la Défense américaine, à une innovation qui a révolutionné l'information, la communication, les relations humaines et sociales, les échanges et la culture [1] . Il existe aujourd'hui une multitude de technologies de l'information et de la communication, particulièrement le réseau internet et les services qu'il propose: réseau sociaux, E-commerce, E-learning, etc. L'avènement des objets connectés est sans doute l'une des innovations majeures de l'internet. C'est une technologie qui regroupe un ensemble d'objets physiques du quotidien intégrés à des capteurs, des logiciels et autres technologies dans le but de collecter des informations et de permettre une communication entre les dispositifs à travers internet offrant ainsi une multitude d'applications et de services. Cette technologie s'intègre de plus en plus dans de nombreux secteurs de la vie quotidienne comme celui de la santé, de l'armée, du transport, de la domotique, etc. et semble ainsi répondre à des usages bien accueillis par le grand public. Ceci incite des milliers de chercheurs et développeurs à travers le monde entier à travailler sur ce domaine en essayant de développer et améliorer cette gigantesque infrastructure d'objets.

L'internet des objets connait donc une expansion fulgurante cependant il présente de nombreux défis qui découlent de ses caractéristiques. Il présente un environnement non maitrisé du fait de la mobilité des objets et des possibilités pour y accéder, une hétérogénéité car les objets peuvent être de nature différente, des ressources limitées en terme de capacité de calcul et d'espace de stockage [2]. Les problèmes liés à la sécurité représentent des défis majeurs qui freinent considérablement l'évolution et le déploiement de l'IoT.

L'authentification est un aspect essentiel pour garantir une bonne sécurité dans les environnements IoT. Les objets traitent et échangent des données sans intervention humaine. Par conséquent, en raison de cette autonomie totale il est primordial de mettre des mécanismes d'authentification pour éviter d'éventuelles menaces. De nombreux chercheurs ont proposé plusieurs types de mécanismes d'authentification d'objets connectés adaptés à l'environnement IoT. La plupart de ces recherches sont basées sur une authentification centralisée selon laquelle tous les dispositifs doivent contacter une certaine entité ce qui

crée un inconvénient majeur. Lorsque l'entité centrale est compromise, le modèle d'authentification est invalide. De tels inconvénients dans la conception de l'IdO peuvent être surmontés en utilisant la technologie blockchain. La blockchain est connue comme la technologie sous-jacente du bitcoin. Elle peut être définie comme un grand livre distribué. Elle permet de remplacer le tiers de confiance par un bloc transparent et non falsifié d'enregistrements disponibles via une forme distribuée, de sorte que la confiance est déplacée d'une entité unique vers des nœuds de blockchain décentralisés. Dans ce travail nous avons étudié la blockchain dans sa globalité mais aussi étudier différents méthodes d'authentifications basées sur cette technologie pour les solutions IoT. Enfin dans la dernière section nous avons proposé un nouveau protocole d'authentification inspiré de la blockchain pour apporter des solutions par rapport aux vulnérabilités des méthodes existantes.

Chapitre I : Internet d'objets

1.1 Introduction

Les technologies de l'IoT se développent à un rythme effréné et offrent un éventail de propositions de plus en plus étendues. L'internet des objets connecte des milliards d'objets et des milliards d'êtres humains. Il peut être considéré comme l'un des outils les plus puissants pour créer, modifier et partager un nombre incalculable d'informations**.** Appelé également Web 3.0, il créé une nouvelle dimension qui enlève les frontières entre le monde réel et le monde virtuel, ouvrant ainsi la voie vers une multitude de scénarios basés sur l'interconnexion entre les deux mondes. Dans ce chapitre nous allons définir l'internet des objets, retracer son historique et son évolution, définir les domaines dans lesquels il est appliqué ; ensuite nous verrons son architecture et écosystème, voir les différents protocoles existants et enfin les défis de l'IoT.

1.2 Définition

IoT (Internet of Things en anglais) ou encore IdO (Internet des Objets en français) peut se définir comme une « infrastructure mondiale pour la société de l'information qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution » mentionne l'Union internationale des télécommunications (UIT) [3].

En ce sens, nous pouvons le définir en terme plus simple comme étant un concept qui permet d'étendre le réseau internet, de pouvoir échanger des données à travers des objets physiques. Il peut s'agir d'objets du quotidien omniprésents dans les logements (télévision, réfrigérateur, machine à laver, système de chauffage, porte de garage électrique), d'appareils ou de systèmes plus complexes comme des véhicules (avions, voitures autonomes) et l'éclairage d'une ville. Ainsi les objets du quotidien deviennent des objets intelligents capables de détecter, d'interpréter et de réagir dans un environnement grâce à l'internet et autres composants comme les capteurs embarqués, la localisation en temps réel ou encore l'identification par radiofréquence.

D'un point de vue conceptuel, l'Internet des objets caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel.

D'un point de vue technique, l'IdO consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http, etc.) d'un objet physique grâce à un système de communication sans fil qui peut être une puce RFID, Bluetooth ou Wi-Fi [4].

1.3 Historique et évolution de l'internet des objets

L'histoire de la technologie de l'Internet des objets a commencé de manière informelle avec une machine Coca-Cola en 1982. C'était un distributeur automatique mis en place au niveau d'une université et que par la suite des étudiants ont innové en y plaçant des capteurs qui vérifient non seulement s'il y a une boisson dans la machine, mais aussi déterminent si elle était froide. Néanmoins ce projet n'a pas dépassé le cadre de l'initiative étudiante.
C'est dans les années 1990 que l'histoire officielle commence avec le grille-pain, les machines à café ou autres objets du quotidien. Le concept même «d'Internet des objets» est officiellement apparu en 1999. Cette phrase a été introduite par le chercheur en technologie RFID Kevin Ashton lors d'une présentation pour Procter & Gamble.

En 2003 l'entreprise Violet propose ce que l'on peut considérer comme étant le premier objet connecté une lampe DAL caractérisée de 9 LED's. Ce dispositif était connecté à internet via WI-FI et pouvait s'allumer de différentes couleurs en fonction des événements liés à la météo, la Bourse, la pollution, les alertes Google ou encore des « envois de messages de couleurs » par sms ou email. En 2005, la même entreprise lance le Nabaztag un lapin connecté en WI-FI qui est considéré comme l'icône des objets connectés [5]. Ce dispositif peut lire des mails à voix haute, diffuser de la musique, etc. (voir la figure 1). Avec l'explosion des smartphones et des tablettes, le nombre d'appareils connectés à internet a atteint 12,5 milliards, en 2010 alors que la population mondiale était de 6,8 milliards [7].
Selon diverses estimations, il y aurait actuellement plusieurs dizaines de milliards d'objets connectés dans le monde durant ces 20 dernières années. Le nombre de dispositifs IoT augmente chaque jour. La raison de cette augmentation du nombre de dispositifs IoT est qu'ils apportent du confort à la vie humaine et effectuent des travaux avec de meilleurs résultats que les humains.
En 2020 l'évolution des objets connectés dans le monde a connu une certaine baisse avec l'apparition de la pandémie ; la COVID 19 qui a entrainé une baisse de 5% du PIB mondial. Mais malgré tous ces faits, le marché de l'IoT a pu

progresser. Les faits montrent que cette technologie est là pour continuer à s'étendre et même à pouvoir apporter des solutions par rapport à la pandémie. Selon les estimations d'IoT Analytics, il y avait en 2020, 21,7 milliards d'appareils connectés actifs dans le monde [8]. D'ici 2025, on s'attend à ce qu'il y ait plus de 30 milliards de connexions IoT, soit près de 4 appareils IoT par personne sur la planète.
L'IoT a joué (et joue toujours) un rôle crucial dans la gestion de la pandémie. Quelques cas d'utilisation centrés sur l'IoT ont joué (et continuent de jouer) un rôle essentiel pour aider le monde à traverser la pandémie. Les plus notables incluent la recherche des contacts basée sur l'IoT sur les lieux de travail, les hôpitaux et ailleurs (Exemple : Concept Reply Tracking & Location System) ainsi que le suivi et la vérification des produits tout au long de la chaîne d'approvisionnement en vaccins.



Figure 1: Nabaztag le lapin connecté [6]

1.4 Domaines d'application

L'IdO permet aujourd'hui d'effectuer des tâches sans la collaboration humaine, ce qui rend la vie simple et facile. Il permet d'automatiser, de réaliser et de contrôler les tâches essentielles à la vie et de fournir de meilleures réponses en conséquence. L'Internet des objets est présent dans presque tous les domaines de notre vie quotidienne :

- La domotique

  La domotique regroupe l'ensemble des techniques et systèmes qui permettent de pouvoir automatiser, programmer et contrôler un habitat. En combinant la domotique les objets connectés et

internet, il a été possible de créer ce que l'on appelle des maisons intelligentes ou smart home en anglais. Une maison intelligente est une habitation dont les éléments par exemple le chauffage, l'éclairage, les alarmes, etc. sont pilotables depuis des applications mobiles sur des smartphone ou tablettes. Il est donc possible de modifier la température, de contrôler l'éclairage ou de vérifier si une personne entre chez l'occupant en son absence. Rendre une maison intelligente apporte ainsi confort et sécurité aux occupants.

- La santé [9]

  L'IoT permet de rendre les organismes médicaux plus intelligents. Il a le potentiel de redéfinir l'interaction et la connexion entre les utilisateurs, la technologie et les équipements dans les environnements de soins de santé afin de faciliter la promotion des meilleurs soins de santé, la réduction des coûts et l'amélioration des résultats. Parmi les solutions IoT dans le domaine de la santé nous avons par exemple les équipements médicaux connectés tels que les scanners de tomographie, des caméras de vidéosurveillance et portes de sécurité avec des lecteurs de cartes d'identité électroniques pour assurer ainsi la sécurité des équipements médicaux portables et surveillance à distance des patients offrant des soins de santé sûrs et efficaces.

- L'agriculture [10]

  L'usage des objets connectés se démocratise dans l'agriculture. Aujourd'hui en pleine transformation, elle se mue peu à peu en smart agriculture. Des capteurs intelligents intégrés dans le sol, sont aujourd'hui capables de signaler aux systèmes d'irrigation la bonne quantité d'eau en cas de besoin ou encore sur la maturité des plantes. D'autres capteurs dans les entrepôts agricoles peuvent fournir des alertes lorsque les conditions telles que la température ou l'humidité dépassent les plages souhaitables. De quoi renouveler en profondeur les pratiques de cette activité ancestrale, grâce à l'analyse des données récoltées et au pilotage de plus en plus fin des exploitations**.**

- Ville intelligente [11]

  Une ville intelligente ou smart city consiste globalement en l'optimisation des coûts, de l'organisation, du bien être des

habitants. Pour développer le concept de ville intelligente, des dispositifs IoT sont déployés pour optimiser divers systèmes et services publics, tels que la gestion des parkings, la gestion des déchets, la gestion du nettoyage, l'éclairage des rues et le contrôle des urgences dans la ville. L'IdO offre ainsi la possibilité de surveiller et de traiter à distance, en temps réel, des données provenant de domaines tels que la communication, les capteurs sur les appareils, la vidéosurveillance, le transport, et les capteurs qui sont situés dans toute la ville.

- Transport [12]

  L'IoT est aussi au cœur de la transformation des transports pour assurer une meilleure sécurité, des voyages plus efficaces, une amélioration de la maintenance des véhicules et des avions mais aussi une gestion plus stratégique du trafic. Parmi les exemples de l'application de l'IoT dans le domaine du transport, nous pouvons citer des transports en commun plus efficaces et moins coûteux, qui se servent des réseaux de capteurs, des caméras numériques et des systèmes de communication pour augmenter la capacité du système et améliorer la sécurité et le confort des passagers tout en réduisant les coûts et les risques.

- Militaire

  Les technologies IoT ont également été utilisées pour des applications militaires et servent de source de valorisation importante pour améliorer l'intelligence des applications militaires. Les sites d'applications militaires comprennent la logistique militaire, la surveillance, et les robots militaires. L'intégration des technologies de l'IdO dans les applications militaires peut contribuer à sauver la vie des personnes en identifiant les produits chimiques toxiques et biologiques.

- Appareils portables [13]

  Concernent les objets dédiés au grand public. Les anglophones le désignent sous le vocable de wearables technology, technologie portable en français. Ce terme désigne tous les objets connectés dont il est possible de se vêtir (vêtements, lunettes, bracelets, montres, bijoux, etc.). Parmi les appareils portables on peut citer les vêtements connectés qui sont pour le moment peu fournis du fait

que leur conception et leur fabrication ne sont pas forcément aisée. Un vêtement connecté peut surveiller l'état de santé d'un bébé ou des personnes âgées, aux combinaisons de sport complètes délivrant des informations sur les rythmes cardiaques et respiratoires. On a aussi des montres connectées qui permettent accéder à des informations utiles à la vie quotidienne d'un simple coup d'œil, interrompre une conversation ou n'importe quelle autre action. Et enfin des lunettes connectées qui augmentent un confort d'utilisation en faisant apparaitre directement toutes les informations utiles juste devant les yeux de l'utilisateur, sans le moindre effort. Il est aussi possible de prendre des photos et vidéos en suivant son regard, ou de se faire guider avec des fonctions de navigation sans avoir à détourner les yeux.

- L'industrie

Le développement d'application IoT est un domaine très actif pour l'automatisation dans le domaine industriel. En effet le concept d'industrie 4.0 fait de plus en plus parler de lui. Elle désigne une nouvelle génération d'usines connectées, robotisées et intelligentes. Ces applications IoT améliorent l'économie globale ainsi que la performance industrielle. Parmi les exemples d'application IoT dans le domaine industriel, nous avons l'intégration de la technologie IoT pour l'apprentissage numérique, la gestion de la chaine d'approvisionnement des produits, la communication machine à machine.

- L'énergie

La raréfaction des ressources, la hausse des prix de l'énergie ou encore l'importance de la protection du climat font que la gestion de l'énergie est l'une des principales préoccupations des entreprises. Pour ajuster la consommation et la production de l'électricité en temps réel dans les réseaux intelligents électriques intelligents (smart grid) par exemple, l'IdO permet une surveillance des informations comme les besoins du réseau, les habitudes et les pics de consommation. Pour cela les capteurs collectent les données grâce à des compteurs intelligents. Les données sont ensuite analysées à l'échelle macro pour en extraire les informations utiles et globales.



Figure 2: Domaines d'application de L'IdO [14].

1.5 Architecture et écosystème

1.5.1 Écosystème IoT

L'écosystème IoT repose sur des objets connectés mais pas que cela, il existe des acteurs bien avant les objets mais aussi après la connectivité. Cet écosystème peut être décomposé en cinq parties [15].

- Chipset : des puces et des modules électroniques qui constituent les capteurs et les transmetteurs et dont l'assemblage compose les objets connectés.
- Objet connecté peut être considéré comme l'objet final constitué des capteurs et des transmetteurs. Ces objets connectés peuvent être à la portée d'une intelligence embarquée et disposent de système d'exploitation pour pouvoir par exemple gérer aux mieux la collecte des données.
- La connectivité qui est le réseau qui va permettre de relier l'objet et d'assurer qu'il puisse échanger ses informations, transmettre les données. La fonction de connectivité est souvent supportée par les réseaux des opérateurs.

- ❖ Plateforme IoT qui est un ensemble de services techniques qui permet le pilotage des objets, la collecte, le stockage, l'analyse et l'exploitation des données envoyées. C'est de drivers de communication, de bases de données, de services de traitements et de calculs et bien souvent un web service pour générer de traitements de bords de visualisation et d'exploitation.
- ❖ L'application utilise les données d'objets connectés et les traduit en information exploitable et mettre en œuvre les données Big Data. Ces applications sont parfois hébergées dans le cloud de manière couplée avec la plateforme IoT choisie.

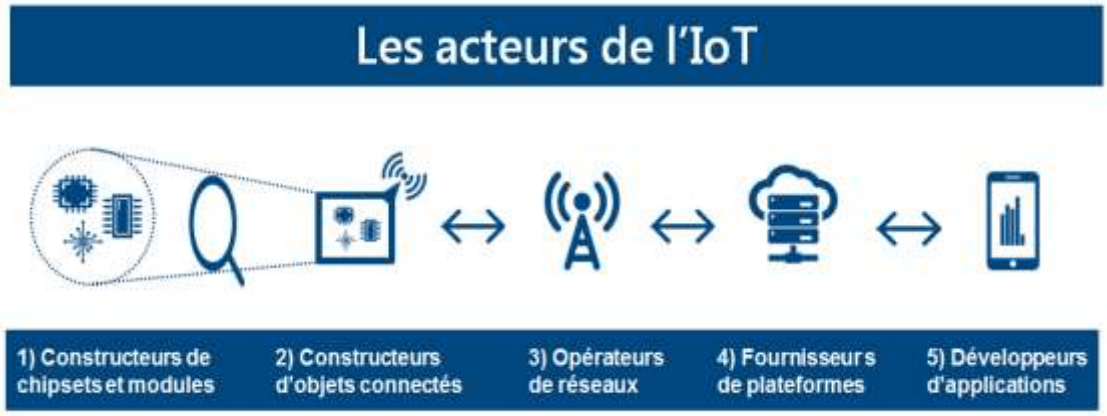


Figure 3: Ecosystème de l'Internet des Objets [15].

1.5.1.1 Domaine des objets connectés

Un objet connecté est un dispositif qui permet de collecter, stocker, transmettre et traiter des données issues du monde physique. Ces objets sont identifiés et identifiables de façon unique. Il existe deux types d'objets :

- ❖ Les objets passifs utilisent le plus souvent un tag (puce RFID, un code barre 2D). Ils embarquent une faible capacité de stockage (de l'ordre de kilo-octet) pour assurer un rôle d'identification. Ils peuvent parfois, dans le cas d'une puce RFID, embarquer un capteur (température, humidité) et être réinscriptibles.
- ❖ Les objets actifs sont équipés de plusieurs capteurs, d'une plus grande capacité de stockage et d'une capacité de traitement. Un objet connecté lorsqu'il communique, il est l'agrégation de 3 voire 4 composantes. Les capteurs qui sont des dispositifs permettant la transformation d'une

grandeur physique observée, exemple la température la pression en une grandeur utilisable comme la tension électrique. Ces dispositifs possèdent au moins un transducteur pour convertir une grandeur physique en une autre ; ou les actionneurs qui sont des dispositifs complémentaires aux capteurs qui convertissent l'énergie électrique en mouvement ou énergie mécanique. Les actionneurs transforment l'énergie reçue en un phénomène physique. Ils existent 3 catégories d'actionneurs : les actionneurs hydrauliques, pneumatiques et électriques. On a ensuite les autres composantes qui sont **:** le vecteur (NFC, RFID, ZigBee, Bluetooth, Wifi), le stockage de la donnée brute, la restitution de donnée traitée**.**

1.5.1.2 Domaine de la connectivité

Une multitude de possibilités existe pour connecter les objets. Cette connectivité est assurée par une petite antenne radio de fréquence au niveau de l'objet pour une communication de l'objet vers un ou plusieurs réseaux. L'identification, l'état ou les données de capteurs des objets peuvent être ainsi remontés mais aussi des informations comme les commandes d'action et de données peuvent être reçues. La connectivité offre aussi une possibilité de pouvoir gérer le cycle de vie de l'objet par rapport à l'authentification et l'enregistrement dans un réseau, la mise en service ou encore la suppression de l'objet. Il existe des dizaines de technologie que nous allons décrire selon la portée.

❖ **Réseaux à courte portée**

Les technologies dans les réseaux à courte portée sont plus utilisées dans la domotique ou sur les wearables.

- Bluetooth

  Bluetooth a été créé en 1994 et a été conçu comme une alternative sans fil aux câbles de données pour l'échange des données via des transmissions radio. C'est le protocole de communication sans fil le plus connu du grand public. Sa consommation d'énergie est faible ainsi que sa portée environ 10 mètres. Il utilise une faible bande passante et possède de nombreuses applications comme écouteurs sans fil, montre intelligente, dans les équipements médicaux, etc.

- Les étiquettes d'identification par radiofréquence (RFID)
  Les capteurs d'identification par radiofréquence permettent une transportation des données grâce à une étiquette RFID et les envoient par les ondes radio à un lecteur RFID qui fait la lecture. Ces puces permettent une localisation précise des produits.
- NFC (Near Field Communication)
  La communication en champ proche (NFC) désigne un ensemble de technologies sans fil de courte portée pour une fréquence de 13,56 MHZ et nécessitant une distance de 4 cm. Cette technologie utilise les mêmes principes que la RFID mais n'est cependant pas utilisée que pour l'identification mais aussi pour la communication bidirectionnelle plus élaborée. Son étiquette peut contenir une petite quantité de données et peut seulement être lue, réinscriptible ou modifiée [16].

❖ **Réseaux à moyenne portée**

- ZigBee
  C'est une technologie de communication radio pour les dispositifs embarqués et constitue un protocol de réseau local (LAN) maillé. Comme le Bluetooth cette technologie possède une large base d'exploitation installée plus dans le secteur industriel. Elle offre des fonctionnalités à faible consommation d'énergie, une sécurité avancée, une robustesse et une grande évolutivité. Elle permet aussi l'exploitation, des réseaux de capteurs et le contrôle sans fil dans l'IoT et les applications machine à machine.
- Z-Wave
  Z-Wave pour désigner une technologie de radiofréquence à faible énergie souvent utilisé dans la domotique, les systèmes de sécurité et les commandes d'éclairages. Ce protocole est utilisé dans les réseaux maillés et permet de transmettre les données à une potée de 30 mètres de base.
- Wifi
  C'est un protocole de communication simple et peu coûteux permettant une connexion à haut débit sur des distances de 20 à 100 mètres des appareils électroniques à internet via des routeurs sans fil. Il est très énergivore et ne peut être utilisé que pour les

appareils branchés sur secteur ou l'alimentation électrique peut être aisée.

- Bluetooth Low Energy (BLE)
  Cette technologie connue sous le nom de Bluetooth smart. Elle fait partie de la pile Bluetooth v4.0. C'est un protocole de réseau personnel qui transmet de petits éléments de données de manière peu fréquente et à faible débit. Contrairement au Bluetooth classique, il est plus allégé et a une portée de 60 mètres.

❖ **Réseaux à longue portée**

- SigFox
  SigFox est un opérateur de réseau IoT mondial. En termes de couverture elle est entre le Wifi et le cellulaire. Il gère les données de 10 à 1000 bps. L'idée de SigFox est que pour de nombreuses applications M2M qui fonctionnent sur une petite batterie et ne nécessitent que de faibles niveaux de transfert de données, la portée du Wifi est trop courte, tandis que le cellulaire est trop cher et consomme beaucoup d'énergie. Il gère de faibles vitesses de transfert de données et ne consomme que 50 microwatts contre 5000 microwatts pour les communications cellulaires [16].
- LoRaWan
  LoRaWan cible les applications de réseau étendu WAN. Sa conception vise à fournir des réseaux étendus de faible puissance. Cette technologie prend en charge la communication bidirectionnelle mobile sécurisée à faible coût dans les applications IoT, M2M et les villes intelligentes. Les débits de données vont de 0.3 à 50 kbps.

- Les réseaux cellulaires (GSM, 2G, 3G)
  Fournis par les opérateurs télécoms, les réseaux cellulaires mobiles permettent de transférer d'importantes quantités de données à une longue portée. Bien que la communication cellulaire (4G en particulier) puisse envoyer de grandes quantités de données, elle implique aussi des coûts et une consommation électrique excessifs pour de nombreuses applications. Elle peut cependant être idéale pour les projets basés sur un capteur et qui,

ne nécessitant qu'une faible bande passante, enverront de très faibles quantités de données sur Internet.

1.5.2 Architecture

L'architecture existante d'Internet avec les protocoles TCP/IP, adoptée en 1980, ne peut pas gérer un réseau aussi important que l'IdO à cause des nombres importants d'objets connectés dans le monde, d'où la nécessité d'une nouvelle architecture ouverte capable de résoudre divers problèmes de sécurité et de qualité de service et de prendre en charge les applications réseau existantes à l'aide de protocoles ouverts. Il est important de définir des standards pour uniformiser la conception des systèmes pour favoriser l'interopérabilité et la communication entre les différents écosystèmes de l'IdO. Mais il n'existe pas d'architecture standard de l'Internet des Objets qui est universellement acceptée. Différentes architectures ont été proposées par différents chercheurs. Ainsi l'architecture d'une solution IoT varie d'un système à l'autre en se basant sur le type de la solution à proposer. Parmi ces architectures, nous avons une Architecture à trois couches, à quatre couches et une autre à cinq couches.

- **Architecture à 3 couches** [17]

  L'architecture à trois couches est l'architecture la plus basique et la plus connue. Elle se compose de trois couches, à savoir les couches de perception, de réseau et d'application (voir figure 4).

  - La couche de perception est la couche physique, qui possède des capteurs pour détecter et recueillir des informations sur l'environnement. Elle comprend notamment des étiquettes RFID, le code-barres bidirectionnel, des capteurs… Ces capteurs sont les composants les plus utilisés dans cette couche. Ils détectent certains paramètres physiques ou identifient d'autres objets intelligents dans l'environnement. Les nœuds de la couche perceptuelle sont généralement limités en termes de capacité de de stockage et puissance de calcul.
  - La couche réseau est considérée comme le réseau neuronal et le cerveau de l'IoT. Elle est responsable de la connexion à d'autres objets intelligents, périphériques réseau et serveurs. Elle permet le transport et la transmission des informations collectées à partir des objets physiques par l'intermédiaire de capteurs. Dans cette couche, la transmission de l'information repose sur plusieurs

réseaux de base, à savoir l'internet, les réseaux de communication mobile, les réseaux satellitaires et les réseaux sans fil. L'infrastructure du réseau et les protocoles de communication sont également essentiels à l'échange d'informations entre les dispositifs.

- La couche application est chargée de fournir des services spécifiques à l'application à l'utilisateur. Il définit diverses applications dans lesquelles l'Internet des objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente.

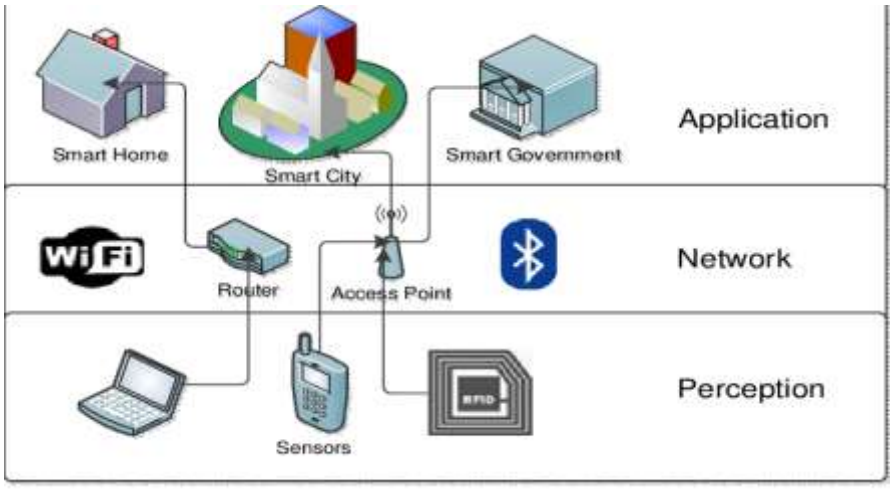


Figure 4: Architecture à 3 couches de l'Internet des Objets [18]

❖ **Architecture à 4 couches** [19]

L'architecture à trois couches précédentes qui est la plus basique en raison du développement continu de l'IdO, ne peut pas répondre à certaines exigences de l'IoT notamment sur la question de la sécurité. En effet les risques de menaces augmentent dans l'architecture à 3 couches du fait que les informations sont envoyées directement dans la couche réseau. C'est ainsi qu'une autre architecture a été proposée. Cette architecture comporte 4 couches dont les trois sont comme celles de l'architecture à 3 couches et ont les mêmes fonctionnalités.

La couche supplémentaire au niveau de cette nouvelle architecture est la couche support. Elle permet de mettre en place une plateforme fiable

pour la couche application. Les plateformes de support comportent des machines de calcul intelligentes qui sont organisées par le biais du cloud computing et de la grille de réseau. Cette couche agit comme un pont entre la couche application et la couche réseau.

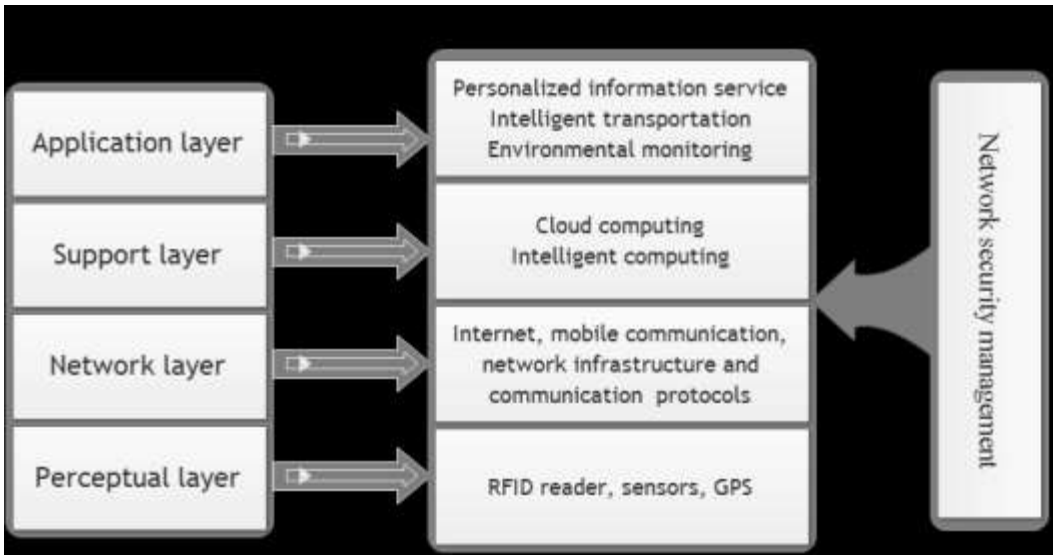


Figure 5: Architecture à 4 couches de l'IoT [19]

❖ **Architecture à 5 couches**

L'architecture à 4 couches a joué un rôle essentiel dans le développement de l'IdO. Cependant les problèmes de sécurité et de stockage n'étaient toujours pas résolus, c'est pour cela que des chercheurs ont proposé une autre architecture à 5 couches. Dans l'architecture à cinq couches, le rôle des couches de perception, de réseau et d'application est le même que celui de l'architecture à trois couches et l'architecture à 4 couches. Les deux couches restantes ont les fonctions suivantes :

- La couche de traitement est également appelée couche middleware. Il stocke, analyse et traite d'énormes quantités de données provenant de la couche de transport. Il peut gérer et fournir un ensemble diversifié de services aux couches inférieures. Il utilise de nombreuses technologies telles que les bases de données, le cloud computing et les modules de traitement de données volumineuses.
- La couche métier gère l'ensemble du système IoT, y compris les applications, les modèles commerciaux et de profit et la confidentialité des utilisateurs.

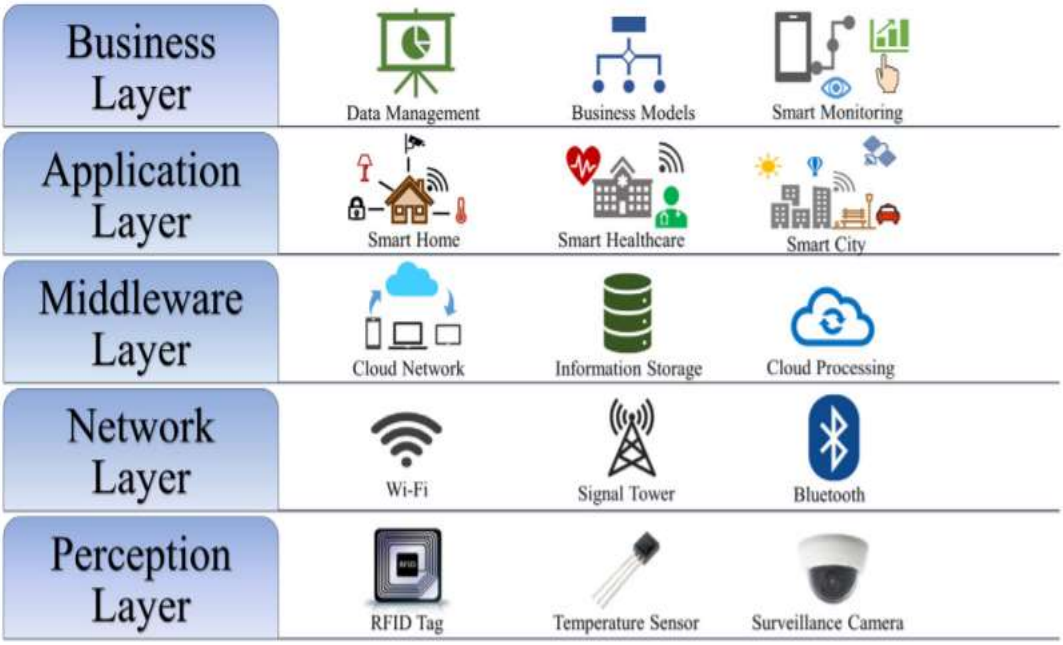


Figure 6: Architecture à 5 couches de l'IoT

1.6 Protocoles

Les protocoles IoT permettent aux appareils IoT de communiquer en garantissant que les informations d'un appareil ou d'un capteur sont lisibles et compréhensibles par un autre appareil, une passerelle, service.
L'environnement contraignant de l'IoT est à l'origine de son problème de normalisation. En effet il est caractérisé par une faible puissance. Une faible exigence en matière de bande passante et une perte de paquets élevée, tout cela ne permet pas une utilisation de la pile TCP/IP. C'est dans ces circonstances que des centaines de protocoles propriétaires dans l'IoT, du M2M et de la domotique (ZigBee et Z-Wave) ont été mis en place pour remédier à ce problème. Un ensemble de protocoles ouverts normalisés a commencé à émerger. Les organismes tels que l'IEEE, l'IETF ou le W3C ont normalisé des protocoles tels que 6LowPAN ou CoAP. Les piles de protocoles IoT normalisées sont représentées à la figure 7 pour chaque couche du modèle TCP/IP [20]. Mais nous nous intéressons aux protocoles de la couche application, transport, internet, la couche liaison de donnée et physique. Les différentes couches des piles de protocoles avec leurs protocoles sont les suivantes :

❖ Au niveau de la couche application qui sert d'interface entre l'utilisateur et l'appareil nous avons les protocoles comme :

- CoAP (Constrained Application Protocol)

  C'est un protocole client/serveur basé sur internet similaire à HTTP conçu pour la communication de périphériques contraints qui possède une faible puissance de traitement dans les communications machine à machine (M2M). Il est conçu pour l'interopérabilité avec le web et les communications asynchrones et s'exécute sur le protocole UDP (User Datagram Protocol).

- MQTT (Message Queue Telemetry Transport)

  C'est un protocole de messagerie spécialement conçu pour la communication machine à machine et la connectivité IoT. Ce protocole est très léger et permet l'envoi des messages de fréquence avec moins de charge utile. MQTT est utilisé par des dispositifs de surveillance embarqués, des capteurs pour une transmission efficace des messages.

❖ Au niveau de la couche transport

Dans cette couche, les protocoles TCP et UDP sont utilisés. TCP est utilisé comme couche de transport sur internet mais la plupart des scénarios IoT, c'est le protocole UDP qui est bien plus adapté car étant plus léger et plus rapide que le TCP. En effet contrairement au TCP, UDP ne dispose pas de fonctions de résilience de TCP telles que la livraison garantie des paquets mais aussi la taille de l'en-tête est beaucoup plus petite que TCP ; ce qui le rend adapté à l'environnement contraint des appareils et des capteurs.

❖ Au niveau de la couche internet

- IPv6

  Le nombre d'appareils connectés à l'IoT est de plusieurs centaines de milliards. Contrairement au système IPv4 qui repose sur des adresses de 32 bits IPv6 permet un adressage de 128 bits ce qui qui augmente considérablement les nombres d'identifiants uniques pour les appareils IoT mais ce

n'est pas tout ce que le nouveau système améliore. IPv6 prend également en charge la configuration automatique, la sécurité intégrée et une variété de nouvelles fonctionnalités de mobilité permettant un degré plus élevé de complexité du réseau. Par contre les dispositifs avec ces adresses IPv6 longues et la manière dont elles s'intègrent dans des trames de liaisons de données petites et légères étaient des défis à relever par des normes. C'est pour cela que l'IETF développe un ensemble de normes de formatage.

- 6LoWPAN

C'est de l'IPv6 sur réseau personnel sans fil à faible puissance (6LoWPAN) et est l'une des premières normes ouvertes définie dans la RFC 6282 de l'IETF largement utilisée dans ce domaine. Elle est capable de faire des encapsulations des en-têtes IPv6 dans de petites trames MAC IEEE 802.15.4 qui ne peut dépasser 128 octets. L'adoption de ce protocole (6LoWPAN IPV6) assure le fonctionnement des protocoles internet dans ces réseaux personnels sans fil à faible puissance qui utilisent la norme IEEE 802.15.4 ; Les principaux avantages de ce protocole est qu'il permet des adressages de longueurs différentes, des topologies de réseau différentes, faible bande passante, une faible consommation d'énergie.

❖ Au niveau de la couche réseau et liaison de l'IdO

La norme de communication sans fil IEEE 802.15.4 normalisée par IEEE définit la couche physique et la couche de contrôle d'accès au support (MAC). Une variété de réseaux personnels sans fil (WPAN) pour diverses applications est détaillée par le groupe 802.15 comme 802.15.1 est pour la technologie Bluetooth. Cette norme se concentre sur la communication à faible ressources telles que l'énergie, la mémoire et la bande passante entre les dispositifs dans un environnement contraint.

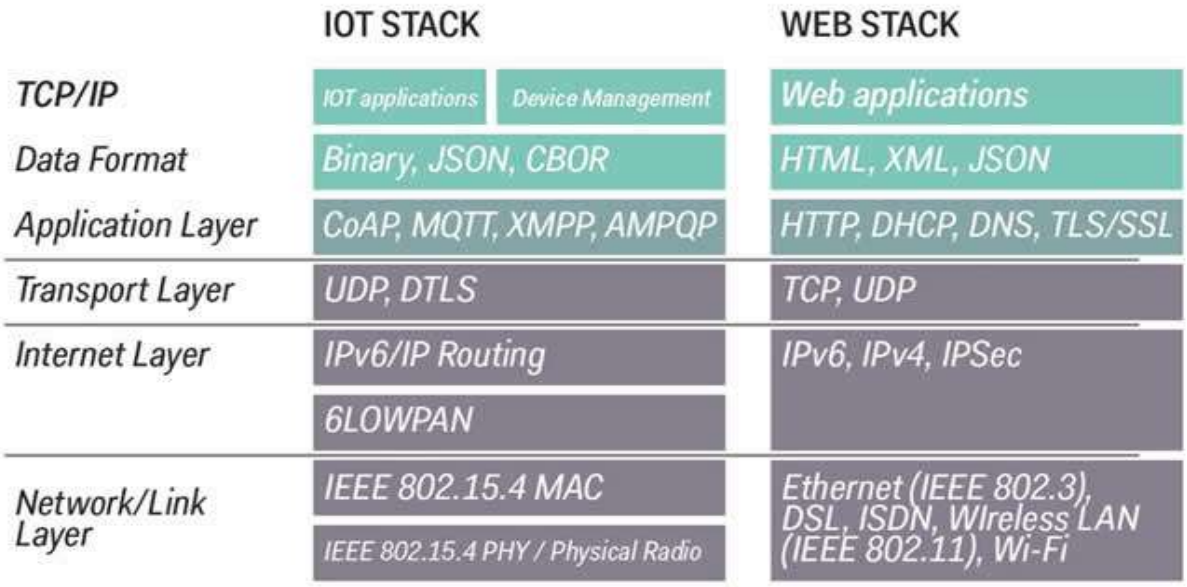


Figure 7: Protocoles réseau IoT mappés sur TCP/IP [21]

1.7 Défis de l'IoT

L'IoT présente de nombreuses limitations qui l'empêchent ainsi d'atteindre son plein potentiel. Parmi les défis de l'internet des objets nous avons [22] :

- Limitation des ressources

  L'écosystème de l'internet des objets compte aujourd'hui de milliards de dispositifs d'une grande variété qui sont connectés à internet. Ces objets sont souvent limités en termes de capacité de traitement, de mémoire mais aussi d'énergie. L'énergie par exemple constitue une ressource essentielle pour les dispositifs intelligents car la plupart fonctionnent par une batterie ou des techniques d'énergie donc les transmissions de données utilisant par exemple les protocoles tels que http ou TCP entrainent le gaspillage de cette énergie.

- Adressage des objets connectés

  L'accroissement du nombre d'objets connectés implique en même temps une augmentation du nombre d'adressage. Le système d'adressage actuel repose sur le protocole IPv4. Cependant le nombre d'adresse disponible pouvant être fournit grâce à ce protocole diminue considérablement. A cette fin un schéma

d'adressage unifié est un domaine de recherche très populaire et un grand défi. De nombreux travaux ont été entrepris pour intégrer IPv6 (qui dispose d'une plage d'adressage beaucoup plus consistant) dans le domaine de l'internet des objets.

- Hétérogénéité

  L'internet des objets est affecté par une grande variété de réseaux, de liens et de dispositifs de connectivité pour fournir différents services. Ainsi différents systèmes d'exploitation et d'interfaces de communication sont utilisés ce qui conduit à une hétérogénéité significative. Cette nature hétérogène joue un rôle critique dans l'interconnexion des dispositifs IoT et constitue un défi à relever. Cette hétérogénéité doit être prise en compte dans les applications IoT afin de permettre l'interopérabilité.

- Grande échelle ou l'évolutivité (scalability)

  L'évolutivité désigne l'augmentation du nombre de nœuds et de réseaux. Elle influence les protocoles de routage ainsi tout schéma de routage doit être suffisamment évolutif pour le nombre de capteurs déployés. L'évolutivité se heurte à une menace ou à un problème critique comme l'attaque par le déni de service, car le plus souvent les solutions IoT sont centralisées et présentent un point unique ou quelques points de défaillance.

- Sécurité

  La sécurité reste le plus grand défi que l'IoT doit surmonter. Des experts en cybersécurité qualifient l'IoT comme étant l'une des technologies les plus vulnérables. En effet les systèmes IoT sont devenus un choix pour les attaquants que ce soit comme cible ou même comme outil d'attaque. Il est donc primordial de pouvoir sécuriser les systèmes. Donc, nous allons dans le chapitre 2, développer les défis, les exigences ainsi que les problèmes en matière de sécurité.

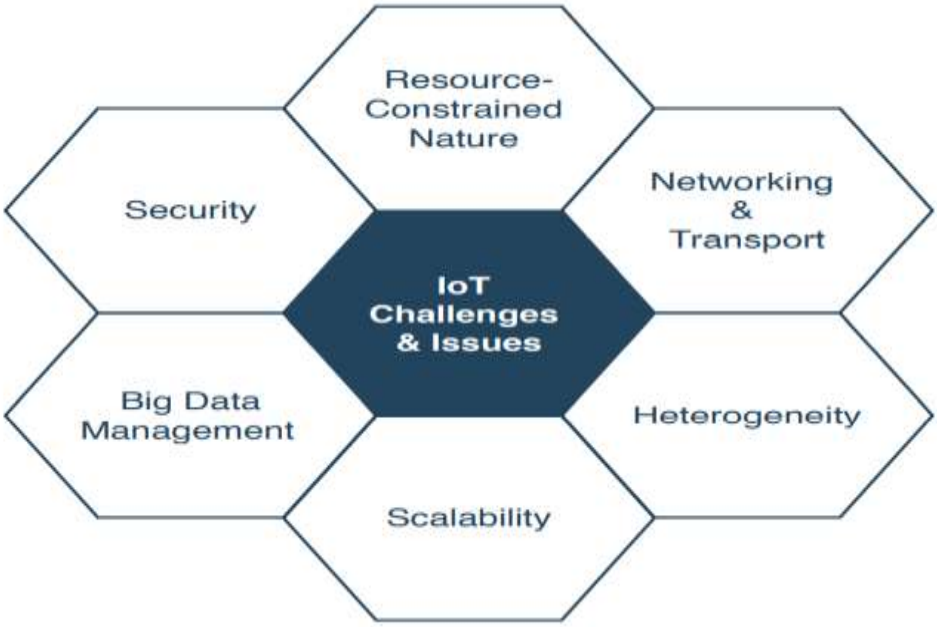


Figure 8: Les différents défis de l'IoT

1.8 Conclusion

L'internet des objets qui a révolutionné le monde, présente de nombreux atouts dans presque tous les domaines de la vie quotidienne. Il existe aujourd'hui plus d'un million d'objets connectés et cette tendance s'accélère. Cette technologie présente cependant de nombreux défis. Les questions d'ordre sécuritaire sont plus que jamais au cœur des attentions. Dans le chapitre qui va suivre nous allons étudier les aspects généraux de la sécurité dans l'IoT.

Chapitre 2 : Les aspects généraux de la sécurité dans l'IoT

2.1 Introduction

Sécurité et technologie ont été toujours intimement liées. Dans la technologie IoT, la sécurité concerne la protection des dispositifs et des réseaux connectés. Elle est devenue l'objet d'un examen minutieux suite à des incidents où un dispositif IoT commun a été utilisé pour infiltrer et attaquer un réseau le plus important. Dans ce chapitre nous allons énumérer les différents services de sécurité, définir les vulnérabilités de l'internet des objets et présenter les différentes attaques auxquels l'internet des objets est confronté.

2.2 Les services de sécurité

La confidentialité :

La confidentialité est la propriété qui assure qu'une information ne peut être lue que par des entités habilitées. Cette propriété est assez importante dans les systèmes IdO, des informations sensibles et confidentielles sont transmises. Il est donc nécessaire de veiller à ce que ces informations ne soient disponibles qu'aux utilisateurs autorisés. Ces utilisateurs peuvent être des êtres humains, des services, des dispositifs internes ou externes aux réseaux. La confidentialité est basée sur le chiffrement des données assuré par des algorithmes mathématiques [23].

L'intégrité :

L'intégrité est la propriété qui assure qu'une information ne peut être falsifiée, modifiée, altérée ou supprimée par une entité non habilitée ou non autorisée[23]. Les données comme nous l'avions si bien précisé tout à l'heure peuvent être sensibles ; exemples des coordonnées bancaires, les enregistrements de factures, etc. Il est primordial que ces données soient protégées et de s'assurer de leur intégrité. L'intégrité des systèmes IoT permet non seulement la protection des dispositifs contre la falsification mais aussi des détections de tentatives de falsification de ces dispositifs. L'intégrité est assurée dans certains cas par des fonctions de hachage et des propriétés de signature de données.

La disponibilité :

La disponibilité est la capacité de rendre un service correct à un instant donné [23]. La disponibilité est une exigence de sécurité par défaut pour toutes les applications de l'IdO et à différentes couches architecturales. Cependant le pourcentage de disponibilité peut varier en fonction des applications IoT et de leur criticité. Pour garantir la disponibilité d'un service, des mécanismes sont utilisés pour une protection contre les arrêts intentionnels des attaques de dénies de service et dénies distribués (Denial/Distributed Denial of service (DoS/DDoS), et non intentionnels.

L'authentification :

L'authentification est le mécanisme qui assure la reconnaissance sûre de l'identité d'une entité [23]. Cette entité peut être un être humain, un programme qui s'exécute ou une machine dans un réseau. Dans le contexte de l'IoT, chaque objet doit pouvoir être identifié (pour disposer de certains privilèges comme de pouvoir envoyer et recevoir des informations ou d'être autorisé à accéder à des ressources) mais doit pouvoir aussi identifier clairement et authentifier d'autres objets. Cependant, ce processus peut être très difficile en raison de la nature de l'IdO (appareils, personnes, services, fournisseurs de services et unités de traitement). Parfois les objets peuvent avoir besoin d'interagir avec d'autres entités la première fois. Il est donc nécessaire d'adopter un mécanisme d'authentification mutuelle entre les dispositifs dans chaque interaction dans l'IdO.

Non répudiation :

C'est la propriété qui assure que l'auteur (utilisateur ou dispositif) d'un acte ne peut dénier l'avoir effectuée. Elle est assurée par des signatures numériques.

Confiance :

Cette propriété consiste à s'assurer que les caractéristiques qu'une entité indiquée concernant sa capacité à remplir certaines tâches et ses propriétés sont bien ce qu'elle prétend et qu'elle peut correctement remplir ces tâches. Elle

consiste également à s'assurer de l'authenticité de l'identité de l'entité. La gestion de la confiance est un processus complexe [23].

Contrôle d'accès :

L'objectif de cette propriété est de pouvoir vérifier la validité d'une autorisation pour l'accès à une ressource protégée. Avec cette propriété, seules les entités authentifiées et autorisées peuvent accéder à une ressource protégée et ainsi permettre de contribuer à la protection de la vie privée des utilisateurs. Il est généralement mis en œuvre par un serveur qui reçoit les requêtes d'accès à une ressource et accorde ou refuse l'accès à l'entité demandeuse. Dans l'IoT, il nécessite une adaptation des mécanismes de contrôle d'accès traditionnels.

2.3 Les vulnérabilités de l'internet des objets

Les attaques qui mettent à mal la sécurité d'un système IoT se basent sur les vulnérabilités de ce dernier. Ces vulnérabilités constituent des faiblesses pour le système. OWAPS (Open Web Application Security Project), un projet ouvert et constitué de divers experts en sécurité pour la sécurité des applications Web à publier un article en 2018 sur les 10 vulnérabilités de l'IoT. Voici 5 exemples de vulnérabilités tirées de cet article [24].

1. Mots de passe : les mots de passe utilisés ne garantissent pas une sécurité sure. Ils sont souvent faibles, devinables ou codés en dur ou publiquement accessibles.
2. Services de réseaux non sécurisés qui compromettent la confidentialité, l'intégrité/authenticité ou la disponibilité des informations ou permettent un contrôle à distance non autorisé.
3. Des interfaces (web, backend API, cloud, mobiles) d'écosystèmes non sécurisés. Les problèmes courants sont l'absence d'authentification/autorisation, l'absence ou la faiblesse de chiffrement et l'absence de filtrage des entrées et des sorties.
4. Transfert et stockage de données non sécurisés : il y a absence de cryptage ou de contrôle d'accès des données sensibles en tout point de l'écosystème y compris au repos, en transit ou pendant le traitement.
5. Absence de mesures de protection physique qui entraine des perceptions de données sensibles et peut entrainer le contrôle de l'équipement localement ou à distance

2.4 Attaques de sécurité

Un attaquant peut avoir plusieurs objectifs comme l'obtention d'un accès au système, l'interruption d'un service, l'envoi d'informations erronées pour induire en erreur des décisions du système etc.

Dans cette section, nous allons présenter quelques types d'attaques qui peuvent nuire aux systèmes IoT. Nous avons classé ces attaques suivant les couches de l'architecture à 3 couches qui est l'architecture la plus basique.

- Les attaques au niveau de la couche perception

  Replay attack ou attaque par rejeu : dans ce type d'attaque, la confidentialité est facilement exploitée en usurpant, modifiant ou rejouant sur les informations d'un dispositif. L'attaquant pourra par la même occasion obtenir la clé de chiffrement en utilisant un autre type d'attaque : l'attaque par temps. L'attaque par rejeu peut occasionner d'autres types d'attaques comme une attaque par capture de nœud qui permet à l'attaquant d'avoir accès à des informations ce qui menace l'intégrité.

  Malicious Node Injection : est une attaque qui consiste à injecter physiquement un nouveau nœud malveillant entre deux ou plusieurs nœuds. L'attaquant aura comme but de modifier les données et transmettre de mauvaises informations aux autres nœuds. Ce type d'attaque dans cette couche peut être comparé à l'attaque de l'homme du milieu ou Man in the middle.

  Malicious Code Injection : Cette attaque est classée parmi les plus dangereuses car l'attaquant peut prendre le contrôle total du système IoT en introduisant un code malveillant dans un nœud du système.

  Physical Damage : Dans ce contexte les dispositifs sont endommagés physiquement et peuvent occasionner un déni de service.

  Social Engineering : Grâce à cette attaque, l'attaquant peut obtenir des informations sensibles en interagissant et manipulant les utilisateurs dans un environnement IoT.

❖ Les attaques au niveau de la couche réseau

Traffic Analysis Attacks : définit une attaque par analyse de trafic et permet à l'attaquant de pouvoir intercepter et examiner des messages pour obtenir des informations sur le réseau.

RFID Spoofing : Cette attaque permet à un attaquant du réseau de falsifier les signaux RFID ensuite il capture les informations transmises par une étiquette RFID. Ces attaques exposent des informations erronées qui semblent correctes et que le système accepte.

Sinkhole Attack : Dans cette attaque, un nœud est compromis à l'intérieur du réseau et l'attaquant pourra envoyer de fausses informations de routage à ses nœuds voisins en disant qu'il possède le chemin de distance minimale vers la station de base. Il pourra ainsi attirer le trafic et par conséquent altérer les données mais aussi abandonner les paquets.

Man in the Middle Attacks : L'attaque de l'homme du milieu sur internet permet d'intercepter la communication entre deux nœuds et d'obtenir des informations sensibles. L'attaquant peut se faire passer pour l'une des cibles, les deux ou rester passif.

Sybil Attack : Pour ce cas, l'attaquant simule l'existence de plusieurs dispositifs qui envoient des informations erronées au serveur ou à l'application de gestion de service pour élire les décisions nécessaires à l'attaquant.

Déni de service : déni de service (DoS) ou une attaque DoS distribuée (DDoS) se caractérise par la tentative de l'attaquant d'empêcher l'utilisation légitime de service. Il existe deux méthodes pour mener une attaque DoS/DDoS par l'exploitation d'une faille de protocole ou par l'inondation de la cible. Ces méthodes font en sorte que les services ne soient pas disponibles pour les utilisateurs prévus.

❖ Les attaques au niveau de la couche Application.

Sur cette couche l'attaquant utilise un virus, un ver, un spyware etc.

Phishing Attacks : l'attaquant obtient des informations privées sur l'utilisateur comme son nom ou encore son mot de passe. Il les obtient en utilisant de faux sites web.

Virus, Worms, Trojan horse, Spyware and Aware (Virus, vers, chevaux de Troie, logiciels espions et logiciels malveillants) : sont des mécanismes utilisés pour les attaques au niveau de la couche application. Des codes

malveillants sont diffusés par le biais de pièces jointes de courriels, de fichiers téléchargeables sur internet etc.

Malicious Scripts : Il est possible pour l'attaquant d'accéder à un système IoT en injectant des scripts malveillants.

Déni de service : L'attaquant s'assure que les utilisateurs sont privés de service sur la couche application.

2.5 Conclusion

Dans ce chapitre nous avons développé les différents aspects de sécurité, présenter les différentes vulnérabilités de l'internet des objets et enfin présenter de façon brève les différentes attaques que l'on peut observer dans l'environnement IoT. Le chapitre suivant mettra l'accent sur un des aspects majeurs de la sécurité en IoT : l'authentification.

Chapitre 3 : Authentification dans l'IoT

3.1 Introduction

Nous avons vu dans la section précédente différentes types d'attaques et des conséquences qu'elles peuvent engendrer notamment sur la vie privée si des informations sensibles sont entre les mains des attaquants. L'authentification des dispositifs, des données et utilisateurs est l'un des principaux services de sécurité à assurer pour garantir un canal de communication sécurisé et fiable. Rappelons que l'authentification permet de vérifier l'identité d'une entité dans le contexte de la sécurité. Elle constitue un facteur clé de succès pour l'IoT c'est dans ce contexte que de nombreux travaux de recherche sur l'authentification des identités des objets connectés ont été menés. Il existe aujourd'hui de nombreux protocoles et schémas d'authentification pour apporter des solutions aux problèmes d'authentification. Un schéma d'authentification sécurisé garantit que les dispositifs ou utilisateurs dans un système IoT sont authentiques. Pour cela, chaque dispositif possède un identifiant unique qui peut être vérifié lorsque le dispositif tente de se connecter au réseau et tout au long du cycle de vie de celui dans le réseau.

Ces schémas d'authentification peuvent prévenir la plupart des attaques de sécurité sur les dispositifs IoT en validant les données de l'utilisateur.

3.2 Taxonomie des schémas d'authentification IoT

Les schémas d'authentification proposés dans les systèmes IoT sont basés sur plusieurs critères. La taxonomie ci-dessous classifie ses différents critères.

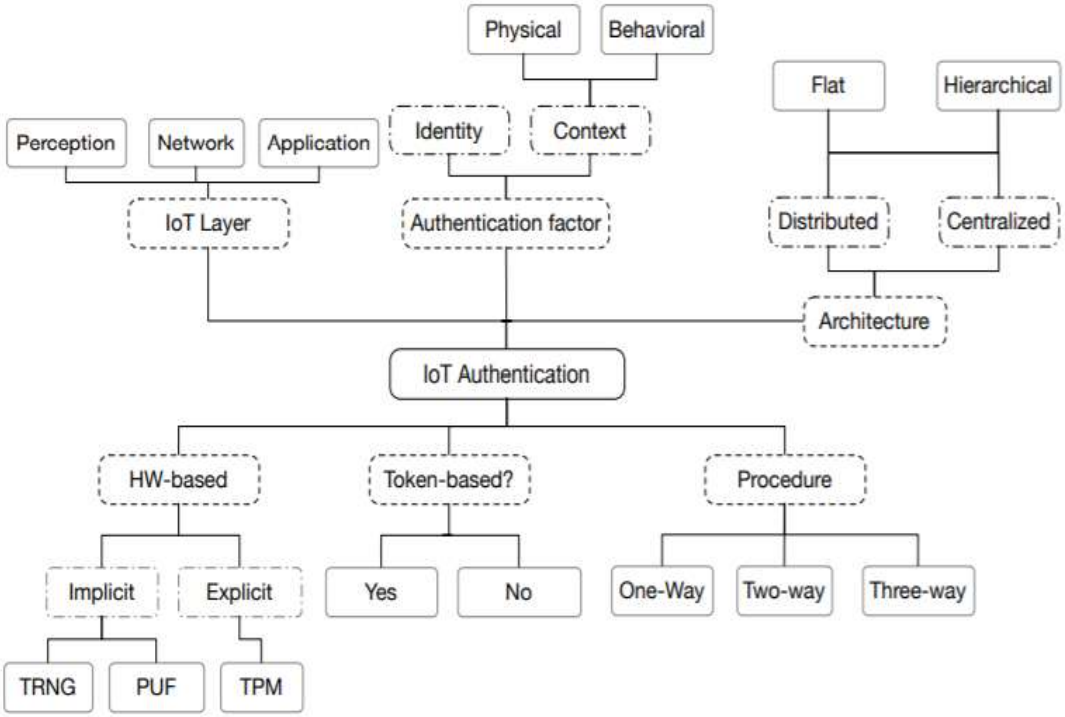


Figure 9: Taxonomie des schémas d'authentification IoT [25]

Authentication factor :

Le facteur d'authentification consiste en deux critères d'identité et de contexte :

- L'authentification de l'identité consiste à envoyer des informations ou des données depuis une entité vers une autre entité pour s'authentifier. Dans ce cas d'authentification, des techniques cryptographiques (asymétriques ou symétriques) ou des fonctions de hachage sont utilisés.
- L'authentification contextuelle par contre consiste en la vérification de l'entité soit par des caractères biométriques physiques ou par des caractères biométriques comportementaux. Pour les caractères physiques, il peut s'agir du scan de la rétine, la reconnaissance faciale ou encore des empreintes digitales, etc. Pour les aspects

comportementaux nous avons par exemple l'analyse de la démarche d'un individu comment il marche, bouge ou court ou encore l'authentification grâce à l'empreinte vocale d'un individu.

Token-based authentication :

Dans ce mécanisme selon la conception des schémas on peut avoir recours ou non à des jetons d'identification pour authentifier les utilisateurs ou les nœuds. Ces jetons sont générés par un serveur. Dans l'authentification sans jeton, c'est plutôt des informations d'identification qui sont prises en compte comme le mot de passe ou le nom de l'utilisateur.

Authentication procedure :

Dans la procédure d'authentification, 3 cas peuvent être présentés. L'authentification unidirectionnelle, bidirectionnelle ou l'authentification à trois voies. Dans l'authentification unidirectionnelle, lorsque qu'une entité veut communiquer avec une autre entité, il doit s'authentifier auprès de celui-ci. Dans celle bidirectionnelle ça sera aux deux entités de s'authentifier chacun à leur tour auprès de l'autre, cette authentification est aussi connue sous le nom d'authentification mutuelle. Enfin dans l'authentification à trois voies, 3 entités entrent en action : deux entités communicantes et une entité centrale (centrale d'authentification). Cette autorité centrale authentifie les deux entités et les aide à s'authentifier mutuellement.

IoT Layer :

Le niveau d'authentification de l'IoT définit la couche (perception, réseau ou application) dans laquelle la méthode d'authentification est mise en œuvre.

Hardware-based :

Le processus d'authentification nécessite aussi l'utilisation des caractères physiques (implicite ou explicite). Implicitement lorsque des caractéristiques physiques du matériel sont utilisées pour améliorer l'authentification exemple avec une fonction inclinable ou un générateur de nombres aléatoires. Basé sur

le matériel explicite comme avec les schémas d'authentification qui font recours à l'utilisation d'un TPM (Trusted Platform Module), un module d'authentification à base d'ADN ou encore une puce qui traite et stocke les clés utilisées pour l'authentication.

Authentication architecture :

L'architecture d'authentification peut être de nature centralisée ou distribuée. L'architecture d'authentification utilise une méthode directe distribuée entre les entités c'est-à-dire que les entités communicantes sont authentifiées avec une authentification directe. Par contre dans les architectures d'authentification centralisée, les entités communicantes vont être authentifiées par une entité centralisée de confiance qui est généralement un serveur ou une tierce partie qui distribue et gère les informations d'identification pour l'authentification. Les deux types d'architectures peuvent être de nature hiérarchique avec plusieurs niveaux pour gérer l'authentification ou de nature plate qui ne nécessite pas de niveaux pour traiter la procédure d'authentification.

D'autres critères peuvent être aussi ajoutés à cette taxonomie telle que les algorithmes cryptographiques utilisés pour les authentifications d'identification. La plupart des services de sécurité reposent aujourd'hui sur la cryptographie avec notamment la confidentialité, l'intégrité, la disponibilité, la non répudiation et bien sur l'authentification. Actuellement les mécanismes de sécurisation utilisent plus la cryptographie comme solution pour régler les problèmes de sécurité. Elle désigne l'étude des algorithmes permettant la protection des informations. Ces algorithmes sont utilisés dans la génération de clés cryptographiques, la signature numérique et la vérification pour protéger la confidentialité des données, la navigation sur Internet, les courriers électroniques et les communications financières confidentielles telles que les transactions par carte de crédit. Le cryptage utilise ces algorithmes appelés chiffrement ou encore cryptosystèmes pour chiffrer (crypter) ou déchiffrer (décrypter) un message. Il existe deux types de cryptographie :

- La cryptographie symétrique ou à clé secrète est une forme de chiffrement rapide basée sur une utilisation d'une seule clé utilisée pour chiffrer et déchiffrer un message. Cet algorithme de chiffrement symétrique part du fait que chacune des parties prenantes dans une communication connait cette clé pré-partagée.

DES, 3DES, AES, IDEA sont des exemples d'algorithmes de chiffrement symétriques. Dans l'IoT, l'AES est plus utilisé comme chiffrement ou l'authentification symétrique.

- La cryptographie asymétrique ou à clé publique est une forme de chiffrement où deux types de clés sont utilisés l'une pour chiffrer et l'autre pour déchiffrer. L'émetteur utilise une clé de chiffrement différente de la clé utilisée par le récepteur pour le déchiffrement. La longueur des clés est de 512 à 4096 bits. Ces algorithmes sont de nature lente car sont basés sur des algorithmes de calcul complexe ce qui fait que les algorithmes symétriques sont à ceux-ci. La cryptographie asymétrique permet non seulement le chiffrement d'informations mais aussi garantie l'authentification des utilisateurs en utilisant la signature numérique à l'aide d'un chiffrement par clé privée et l'utilisation des certificats numériques. Les clés asymétriques sont générées par paire. La clé publique est extraite et publiée à travers des annuaires, par exemple, tandis que la clé privée est gardée secrète chez l'utilisateur (dans mémoire). Exemples de d'algorithmes de chiffrement asymétriques : RSA, ECC, Deffie-Hellman, etc. L'ECC s'impose comme algorithmes de chiffrement dans l'IoT.
- Les algorithmes de hachages permettent d'assurer l'intégrité et l'authenticité des messages. Un algorithme de hachage prend un message donné et génère un condensé appelé HASH ou empreinte. Ils fournissent une preuve d'authenticité quand il est utilisé avec une clé secrète. Exemple d'algorithmes de hachage MD5, SHA-256.SHA-512.

La cryptographie est largement utilisée pour sécuriser les systèmes d'information ; cependant dans le domaine de l'IoT, elle se heurte à un triple obstacle qui est la puissance de calcul, la capacité de mémoire disponible ainsi que la consommation électrique des objets connectés. En effet la cryptographie consomme beaucoup de ces ressources. Les différents types d'algorithmes (symétriques et asymétriques) ne répondent pas aux exigences de performance, de consommation et d'empreinte mémoire, c'est pour cela que de nouveaux algorithmes dits légers sont de plus en plus mis en œuvre.

3.3 Exigences sur les schémas d'authentification dans l'IoT

Les schémas d'authentification doivent satisfaire un certain nombre de paramètres dans l'IoT vu les contraintes liées aux dispositifs. Parmi ces exigences nous pouvons citer :

- Les systèmes d'authentification doivent être légers car les dispositifs IoT ont pour la plupart une faible puissance de calcul, une consommation d'énergie faible et une capacité de stockage limitée.
- Les systèmes d'authentification doivent garantir une authentification multifactorielle. Un seul facteur comme par exemple un nom d'utilisateur ou un mot de passe ne peut garantir une sécurité adéquate. Ainsi ces systèmes en d'autres termes doivent être robustes.
- Tout système doit être aussi efficace car l'authentification à plusieurs facteurs peut surcharger les dispositifs de détection.
- Les systèmes d'authentification doivent combiner les techniques cryptographiques comme le RSA, l'AES et d'autres plus avancées comme la courbe elliptique (ECC) et le hachage.

3.4 Les défis des schémas d'authentification dans l'IoT

De nombreuses approches ont été proposées pour l'authentification des dispositifs et l'intégrité des données dans l'IdO. Exemples :

Dans [26], les auteurs proposent un cadre basé sur l'apprentissage automatique pour l'authentification des dispositifs IoT. Dans l'article [27], les auteurs proposent un schéma d'authentification mutuelle léger qui valide l'identité des dispositifs participants avant de les engager dans la communication.

La plupart des approches proposées prouvent leur robustesse, leur légèreté ainsi que leur efficacité en termes de consommation d'énergie. Cependant la plupart de ces mécanismes classiques d'authentification et de sécurité sont centralisés et nécessitent un tiers de confiance qui peut être un serveur par exemple. L'authentification fonctionne à la base sur la gestion des identités (c'est avec une identité qu'on peut authentifier). Le risque que ces mécanismes soient centralisés est qu'il existe un point de défaillance unique et les utilisateurs doivent faire confiance à ce serveur. En effet, si dans une attaque de par déni de service (DoS ou DDoS), la cible est le nœud central du système, la défaillance du nœud (blocage ou perturbation de son fonctionnement) affecte l'ensemble du système.

Le fait que ces approches soient centralisées pose aussi un problème d'évolutivité. Dans leur article (Atlam et al, 2018), Atlam et al. défendent l'idée que le passage de l'IoT à un système décentralisé pourrait être une bonne voie pour résoudre de nombreux problèmes, notamment en termes de sécurité. Par ailleurs, Brody et al. (Brody et al. 2014) soutiennent que, pour être rentable et durable, l'écosystème d'appareils IoT qui ne cesse de croître devrait évoluer vers une architecture décentralisée réduisant ainsi les coûts de maintenance pour les fabricants et renforçant la confiance des utilisateurs [28]. Pour surmonter ces problèmes, de nombreux travaux de recherche ont préconisé l'utilisation de la technologie blockchain, car ses caractéristiques peuvent apporter des solutions prometteuses à divers problèmes de sécurité de l'IdO.

Elle a été développée sur la base de la vision de la création d'un système décentralisé, distribué et crypté qui peut prendre le relais du système de stockage organisationnel central traditionnel et doit rendre les transactions possibles directement entre les participants du réseau.

3.5 Conclusion

Ce chapitre présente la taxonomie des schémas d'authentification dans les systèmes IoT ainsi que leurs exigences. Mais surtout ce chapitre met l'accent sur les défis à relever dans le contexte de l'authentification avec notamment des problèmes qu'engendrent les méthodes d'authentification centralisées. Dans le chapitre suivant, nous allons nous intéresser à la technologie blockchain qui est une technologie décentralisée et qui pour de nombreux chercheurs vient apporter des solutions aux environnements IoT notamment par rapport à l'authentification des dispositifs IoT.

Chapitre 4 : Blockchain

4.1 Introduction

Le concept de Blockchain a d'abord été conçu comme une technologie habilitante pour le système cryptographique Bitcoin, présenté en 2008 par un mystérieux personnage appelé Satoshi Nakamoto (Nakamoto, 2008). Cependant, rapidement - dans un laps de temps très court - la blockchain, en raison de ses vastes possibilités d'application dans de multiples domaines, a prouvé de manière significative son caractère distinctif en tant que technologie autonome. En fait, on peut affirmer que la Blockchain elle-même n'est pas une nouvelle technologie mais plutôt un nouveau concept d'utilisation de différentes technologies existantes dans une approche incorporée.

4.2 Définition

Blockchain est défini de manière générale comme étant une « technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ». Le terme blockchain désigne une chaine de blocs sur lesquels sont stockées des données de toute nature. C'est une base de données partagée (entre les nœuds du réseau) qui enregistre chronologiquement des transactions et contient ainsi l'historique de tous les échanges effectués entre de utilisateurs depuis sa création.

Cette technologie est de type registres distribués DLT (Distributed Ledger Technology) connu aussi sous le nom de registre partagé et s'appuie sur un réseau de pair à pair qui fait qu'elle est totalement décentralisée. Chaque nœud dans ces réseaux conserve une copie du grand livre afin d'éviter un point de défaillance unique. Toutes les copies sont mises à jour et validées simultanément.

L'écosystème Blockchain utilise de manière significative des mécanismes de hachage mathématique et de cryptage à clé asymétrique pour la sécurité des données ainsi qu'une approche de consensus basée sur les nœuds P2P pour l'immuabilité [29].

4.3 Origine

En 2008 apparue la première blockchain, il s'agit d'une cryptomonnaie lancée par une ou plusieurs personnes dont l'identité n'est connue que par un

pseudonyme : Satoshi Nakamoto. Il posait ainsi les bases de la première monnaie électronique mondiale sur laquelle aucune autorité ne pouvait exercer son contrôle. Cette monnaie virtuelle appelé Bitcoin a été conçue pour répondre aux problèmes de complexité, de vulnérabilité, d'inefficacité et de coût des systèmes de transactions existants. Tels que PayPal, VISA ou encore Master.

En effet ces méthodes traditionnelles de transactions peuvent être :

- ❖ Très coûteuses car elles englobent des intermédiaires qui facturent des frais pour leurs prestations
- ❖ Inefficaces avec des délais assez longs pour l'exécution des contrats et des actions redondantes nécessaires pour tenir plusieurs registres.
- ❖ Vulnérables car si un système central tel qu'une banque subit une atteinte exemples une fraude, une cyberattaque ou une simple erreur, l'impact touche l'ensemble du réseau d'entreprises [30].

Avec la blockchain, les internautes peuvent réaliser des transactions sécurisées de pair à pair, sans que l'intervention d'une tierce partie soit nécessaire pour garantir leur intégrité.

4.4 Caractéristiques de la blockchain

La décentralisation : Contrairement aux systèmes de transactions centralisées classiques, la blockchain est un système de bases de données décentralisé qui permet aux utilisateurs d'avoir un accès libre. Les données peuvent être consultées, surveillées, stockées et mises à jour sur plusieurs systèmes. Une transaction dans le réseau blockchain peut être effectuée entre deux pairs (Peer-to-Peer) sans l'authentification par l'agence centrale. De cette manière, la blockchain peut réduire considérablement les coûts des serveurs (y compris les coûts de développement et les coûts de fonctionnement) et atténuer les goulots d'étranglement au niveau du service central.

L'immuabilité **:** cet attribut constitue l'une des caractéristiques les plus importants de la blockchain. Elle consiste à ce que les données, une fois insérer dans les blocs, ne peuvent être modifiées ou altérées par la suite. Le système cryptographique de validation garantit qu'il est quasiment impossible de réécrire une transaction une fois son bloc validé.

Une transparence et une traçabilité : la blockchain est qualifiée de transparente car tout le monde peut la télécharger dans son intégralité et vérifier à tout moment son honnêteté. Tous les utilisateurs de la blockchain peuvent ainsi voir les transactions présentes et passées. Ils peuvent facilement vérifier et retracer les transactions validées grâce à l'horodatage.

Anonymat**:** l'identité de l'individu reste anonyme lorsqu'il y a transfert de données entre les nœuds. Chaque utilisateur interagit avec le réseau avec une adresse générée. Il est possible qu'il génère plusieurs adresses pour éviter l'exposition de son identité.

Autonomie : Le système blockchain est indépendant et autonome. Chaque nœud du système blockchain peut accéder aux données, les transférer, les stocker et les mettre à jour en toute sécurité, ce qui les rend fiables et exemptes de toute intervention externe.

4.5 Structure d'une blockchain

Comme son nom l'indique la blockchain est une chaine de blocs qui sont liés de manière sécurisés grâce à la cryptographie. En général chaque bloc contient les composants suivants : un hachage cryptographique du bloc précédent, un horodatage et des données de transaction. Les blocs sont reliés entre eux pour former une chaine et chacun de ces blocs fait référence au bloc précédent dans la chaine. Le tout premier bloc dans une blockchain est appelé nœud de genèse

La figure suivante illustre la structure de la blockchain qui est décrite comme suit :

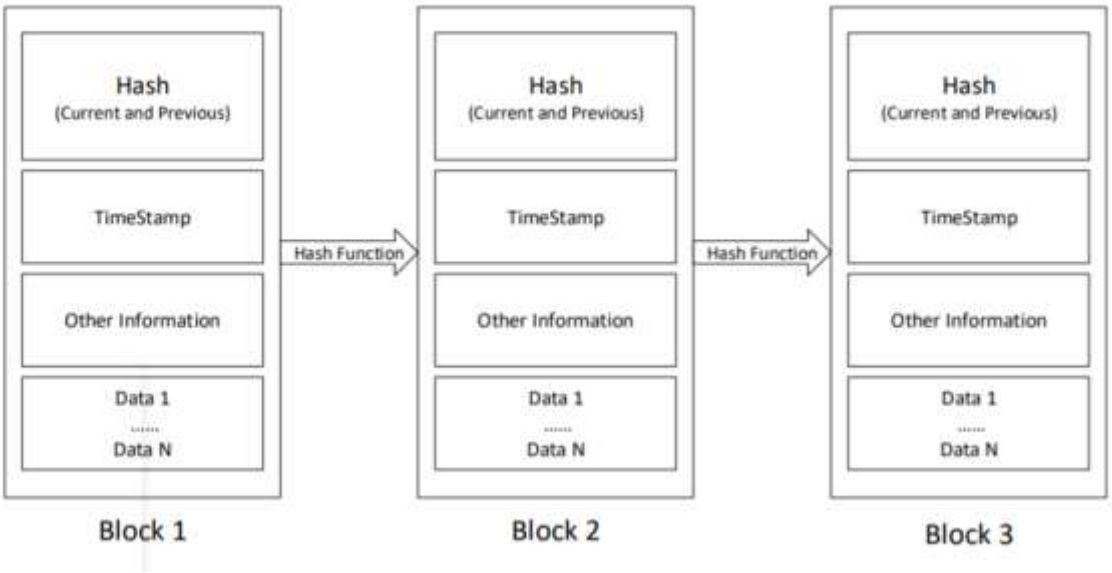


Figure 10: Structure d'une blockchain

- Les données de transaction sont stockées dans la blockchain. Elles peuvent être de n'importe quel type, comme des transactions monétaires, des données de santé, des journaux système, des informations sur le trafic, etc.
- Un hash pour l'identifiant du bloc et le hash du bloc précédent. Ces fonctions de hachage prennent n'importe quelle longueur en entrée et génère en sortie une longueur fixe unique. Si une seule valeur est modifiée la sortie sera différente. Chaque bloc contenant des données est haché et les modifications peuvent être grandes ou petites.
- Horodatage ou TimeStamp en anglais pour enregistrer l'heure à laquelle un bloc a été créé. La présence d'un horodatage pour une transaction va permettre de certifier l'antériorité d'une information sur une autre et donc de pouvoir ordonner les transactions dans un environnement décentralisé.

D'autres informations telles que les signatures numériques, des valeurs de nonces, des nBits et quelques autres valeurs sont définies par l'utilisateur. Les utilisateurs dans ces réseaux signent leurs transactions grâce à des clés cryptographiques publiques et privées lors de la phase de signature et de la vérification. La clé privée est gardée confidentielle et est utilisée pour signer une transaction et crypter les données. La clé publique est connue de tous et est utilisée pour valider et décrypter les données dans la phase de vérification de la

transaction, confirmant ainsi l'authenticité des données. Une valeur de nonce est essentiellement une valeur de 4 octets commençant par 0 et s'incrémente chaque fois qu'un calcul de hachage est effectué. La valeur n bits détermine la valeur seuil cible d'un hachage de bloc valide.

4.6 Fonctionnement du réseau

Une blockchain est déployée sur un ensemble d'ordinateurs qui constituent les nœuds du réseau. Les nœuds peuvent être divisés en deux groupes. Nous avons les nœuds complets qui contiennent une copie complète de la blockchain et les nœuds légers qui hébergent une version minimale de la blockchain leur permettant de participer aux échanges sur le réseau. Le Fonctionnement du réseau peut être résumé comme suit :

Un utilisateur demande une transaction. La transaction est diffusée sur un réseau P2P public (réseau Blockchain) composé de plusieurs nœuds. Le réseau de nœuds va ensuite valider la transaction avec un algorithme de hachage. Une fois vérifiée, la transaction est combinée avec d'autres transactions pour créer un nouveau bloc de données pour le grand livre. Le nouveau bloc est ajouté et horodaté à la chaîne de blocs existante sous une forme qui est permanente et inaltérable. Enfin la transaction sera effectuée avec succès.

Afin de prouver la validation honnête des blocs, il existe de nombreux mécanismes de consensus. Dans la suite nous allons présenter quelques mécanismes de consensus bien connu [31].

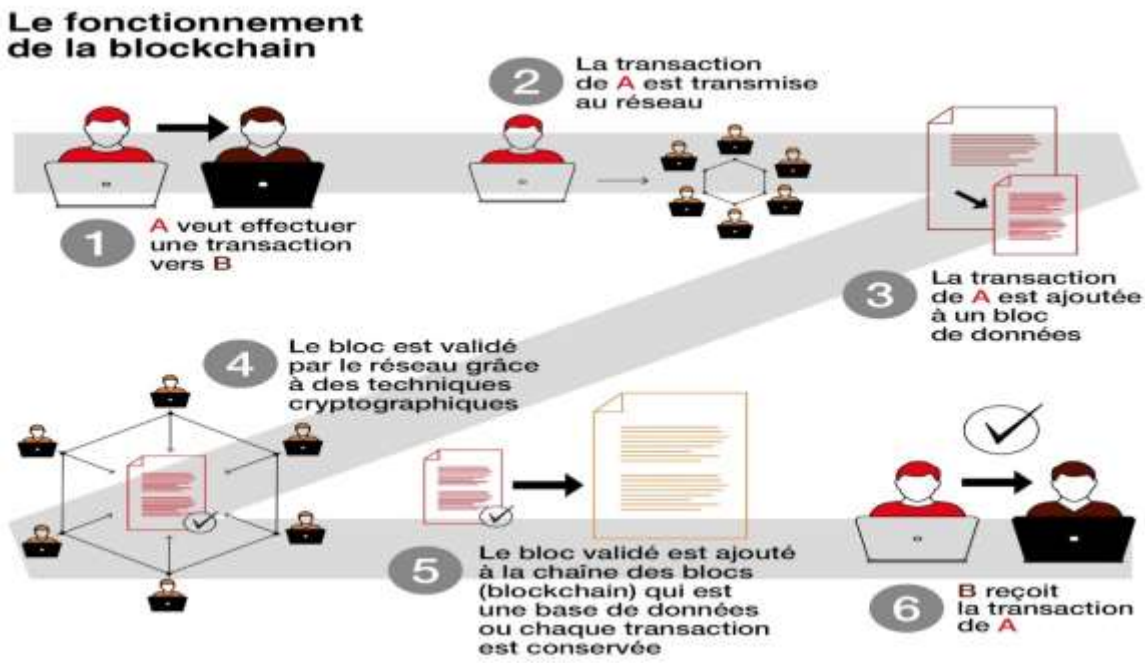


Figure 11: Fonctionnement de la blockchain [32]

4.7 Mécanismes ou algorithmes de consensus

Dans un réseau blockchain, pour que les nœuds puissent s'accorder sur la validité d'un bloc, ils doivent s'appuyer sur des algorithmes de consensus. Ces algorithmes permettent d'établir les conditions dans lesquelles une transaction ou un échange d'actifs peut avoir lieu. Parmi les mécanismes de consensus nous pouvons citer [33] :

1. Preuve de travail ou Proof of work en anglais est le résultat du problème cryptographique à résoudre pour qu'une nouvelle information soit ajoutée dans un bloc. Les blockchains étant des bases de données et des systèmes d'échanges se développent par le contrôle, la validation et l'ajout de nouveaux blocs à leur chaine. Pour ce faire, ce sont les membres du réseau eux-mêmes qui effectuent le travail de vérification et d'adjonction. Dans le cadre de la preuve de travail, ces membres actifs sont appelés mineurs. Ces mineurs effectuent, d'une part, la conformité des données entrantes et d'autre part fournissent la preuve de travail. Pour fournir cette dernière, les mineurs procèdent au minage en calculant le hash d'un nouveau bloc potentiel à partir des données dudit bloc et de la variable nonce. Ce résultat est assez difficile à trouver, cette complexité de calcul vise à sécuriser au maximum le système. Cependant la PoW consomme une grande quantité d'énergie lors de la résolution du défi

mathématique, ce mécanisme peut mener à une potentielle tragédie des ressources d'usage commun. En effet, plus la blockchain ne se développe, plus les preuves de travail nécessitent des calculs longs et énergivores. Le mineur qui aura un matériel informatique assez puissant (dans le cas d'une longue blockchain) et qui aura en premier fournit la preuve de travail au reste du réseau obtiendra une récompense sous forme de tokens dans la cryptomonnaie correspondante. Parmi les cryptomonnaies utilisant ce cryptomonnaie nous avons le Bitcoin.

2. La preuve d'enjeu (Proof of Stake)

   La PoS a été proposé pour résoudre les lacunes de la PoW. Dans ce mécanisme, il n'y a pas de minage qui nécessite des calculs complexes et énergivores. Les membres actifs du réseau sont appelés minters (forgeurs en français). Avec la PoS, pour valider un bloc, les forgeurs mettent en jeu une certaine quantité de jetons en leur possession. Plus le forgeur possède de monnaies, plus il aura la chance de valider un bloc. Il recevra une récompense en jeton à chaque validation. Le fait de confier la validation des blocs aux nœuds les mieux pourvus de jetons garantit la sécurité du système. En effet la conformité des données est capitale pour les forgeurs qui se verraient pénaliser s'il y a une défaillance sécuritaire : la valeur de leur jeton chute à chaque fois que le bloc est taxé de malhonnête. Le point de défaillance de ce mécanisme réside sur le fait que seuls les forgeurs qui possèdent plus de jetons en bénéficient le plus.

3. La preuve d'enjeu déléguée (Delegated Proof of Stake)

   La DPoS est un mécanisme de validation de bloc démocratiquement représentatif c'est-à-dire que les parties prenantes élisent des délégués pour générer et valider les blocs.

4. Il existe d'autres types d'algorithmes de mécanisme de consensus utilisant les variantes de Tolérance aux fautes byzantine (BFT) : Practical Byzantine Fault Tolerance (PBFT) est la première solution pratique pour atteindre le consensus face aux défaillances byzantines, PBFT est un algorithme de consensus utilisé dans Hyperledger Fabric. CrossFault Tolerance est un protocole qui simplifie le modèle d'attaque et rend la tolérance de panne byzantine réalisable et efficace pour des scénarios pratiques. Ripple et Stellar sont deux plates-formes basées sur des blockchains et des protocoles de paiement qui utilisent des variantes de la tolérance de panne byzantine en les rendant ouverts à la participation des nœuds.

4.8 Plateformes Blockchain

Le nombre de plateformes blockchain est élevé et en constante évolution. Trois plateformes seront ici présentées qui sont les plus populaires et les plus adaptées aux domaines de l'IdO. [34]

1. Le Bitcoin est la première cryptomonnaie et la première plateforme blockchain, il permet d'effectuer des transactions monétaires de manière rapide, bon marché et fiable. Il peut être intégré dans des applications en tant que système de paiement sécurisé. Dans le domaine de l'IdO, les appareils autonomes peuvent utiliser les bitcoins pour effectuer des micro-paiements fonctionnant principalement comme des portefeuilles.
2. Ethereum est considérée comme la blockchain la plus prometteuse après Bitcoin. Il est considéré par ses créateurs comme le " premier véritable ordinateur mondial ". Elle permet de fournir une crypto monnaie appelée Ether (ETH). Cette blockchain est utilisée pour effectuer des transactions financières ainsi que le traitement d'autres types de données. En plus de la validation des blocs, les nœuds actifs d'Ethereum traitent des programmes appelés Smart Contracts. Un contrat intelligent est un programme informatique composé d'un ensemble de règles exécutées sur la blockchain. L'inclusion de contrats intelligents éloigne ainsi la blockchain des monnaies et facilite l'intégration de cette technologie dans de nouveaux domaines. C'est pourquoi Ethereum représente une plateforme pour les applications décentralisées. Les contrats intelligents sont exécutés par les objets participants à l'aide d'un système d'exploitation appelé Ethereum Virtual Machine (EVM).
3. Hyperledger Fabric
   Hyperledger est une plateforme open-source sur laquelle divers projets liés à la blockchain ont été développés dont hyperledger fabric qui repose sur une architecture modulaire offrant des degrés élevés de confidentialité, de résilience, flexibilité et d'évolutivité. Elle est conçue pour prendre en charge des implémentations enfichables de différents composants et pour s'adapter à la complexité et aux subtilités qui existent. Néanmoins, il a des limites, par exemple les applications construites sur Hyperledger ne peuvent pas être entièrement décentralisées et seront moins évolutives.

4.9 Types de Blockchain

Il existe 3 types de blockchain [34]

- Blockchain publique est un grand livre public (sans permission), ouvert à tous ou n'importe qui peut rejoindre le réseau et est en mesure d'effectuer une transaction ou de prendre part au processus de consensus entre l'ensemble des nœuds distribuées afin d'ajouter un nouveau bloc au registre. Toute personne disposant d'un ordinateur et d'une connexion internet peut être inscrit en tant que nœud et peut recevoir l'historique complet de la blockchain. Bitcoin et Ethereum sont de types blockchain publiques.
- Blockchain privée est une blockchain restreinte c'est-à-dire qu'elle a une gestion stricte en ce qui concerne l'autorité d'accès aux données. Elle n'est accessible que sur invitation et tous les membres du réseau se connaissent et se font confiance. Les nœuds du réseau ne peuvent pas participer à la vérification ainsi qu'à la validation des transactions. Tout ceci sera assuré par une organisation ou une entreprise qui va initier, vérifier et valider chaque transaction. Hyperledger (de Linux Fondation) et Ripple sont des exemples de blockchains privées.
- Blockchain permissionnée ou encore Consortium Blockchain est une combinaison de blockchain publiques et privées. Seuls quelques nœuds prédéterminés pourront vérifier et valider les transactions ou les blocs. Cependant toutes les transactions sont publiques. Le droit de lecture peut être public ou limité aux participants. Les Blockchains du consortium préservent la confidentialité des données, comme les Blockchains privés. BigchainDB est un exemple de consortium Blockchain.

4.10 Domaines d'application

La technologie Blockchain a lentement mais régulièrement superposé sa position dans tous les domaines.

Domaine financier :

Initialement la blockchain a été développée comme l'épine dorsale pour la monnaie numérique décentralisée : le Bitcoin. Mais de nos jours, il existe plusieurs autres monnaies numériques qui utilisent la structure de la blockchain

avec différents consensus pour vérifier et valider des blocs comme Peercoin, Ethereum, Hashcash, etc.

Domaine sanitaire :

La blockchain offre de nouvelles opportunités stimulantes pour le secteur des soins de santé. En effet, elle peut créer un contexte électronique dans lequel les transactions commerciales (telles que les initiatives de partage d'informations) ente les parties sont menées via une communauté distribuée plutôt qu'une autorité centrale ou une entité unique. La blockchain peut aussi faciliter l'échange d'information et la coordination entre les entités de soins de santé et aider les patients à devenir indépendants dans le partage de leurs Dossiers médicaux avec les prestataires.

Application mobile :

Les développeurs d'applications utilisent la technologie blockchain pour rendre les paiements numériques plus accessibles, faciles et sécurisés. La nature des transactions peer-to-peer en fait une solution idéale pour les applications bancaires qui ont besoin d'un tel type de technologie. Ils existent plusieurs types d'applications mobiles basées sur la blockchain comme les applications pour échanger des cryptomonnaies, des portes feuilles électroniques, etc.

Domaine de la défense :

Dans les domaines spécifiques à la défense, l'utilisation de blockchains privées et cryptées peuvent notamment permettre l'enregistrement et le partage de données ayant un besoin d'intégrité extrême (plans d'opérations, ciblage, règles d'engagement, plans d'infrastructures sensibles…) ou à fort besoin de traçabilité (suivi des effectifs, de l'armement, etc. mais encore de la situation logistique en opérations, ou des configurations informatiques).

Domaine de l'automobile :

La blockchain vise à rationaliser l'industrie automobile en lui garantissant plusieurs avantages :

Avec les voitures qui deviennent de plus en plus connectés et de plus en plus vulnérables la blockchain grâce à ses racines cryptographiques, rehausse le niveau de sécurité, en rendant le véhicule et les données s'y trouvant infranchissables, même en cas de cybercriminalité. La blockchain peut prendre en charge le processus de fabrication, le stockage des données de connaissement pour les composants de la voiture, les rapports d'inspection qualité, et plus encore.

Dans le domaine de l'IoT [35] :

La technologie blockchain est une révolution dans les systèmes d'enregistrement et a été prévue par l'industrie et la communauté des chercheurs comme une technologie émergente qui peut jouer un rôle important dans la surveillance, le contrôle et surtout la sécurisation des dispositifs IoT**.** L'application de la technologie blockchain dans le système de l'IoT offre de nombreux avantages. Elle offre une architecture décentralisée permettant une amélioration de la tolérance aux pannes, une extensibilité ou une évolutivité du système IoT. La blockchain est capable de fournir une authentification et une autorisation distribuées fiables des nœuds pour les applications IoT. Les dispositifs sont capables d'interagir les uns avec les autres sans l'intervention de serveurs et garantissent ainsi une autonomie. Une certaine fiabilité est aussi garantie car les informations de l'IdO peuvent rester immuables et distribuées au fil du temps dans la blockchain. Les participants au système sont capables de vérifier l'authenticité des données et ont la certitude qu'elles n'ont pas été altérées.

Malgré ces nombreux avantages, la blockchain présente cependant quelques inconvénients par rapport aux écosystèmes IoT

Par rapport au stockage : Le grand livre numérique sera stocké sur chaque nœud IoT et au fur et à mesure sa taille de stockage augmentera ce qui sera une tâche difficile car la plupart des nœuds connectés IoT sont limités en terme de stockage de données. D'autre part aussi dans l'IoT, des appareils peuvent générer des giga-octets de données en temps réel, cette limitation représente un grand obstacle à son intégration avec la blockchain. En effet, certaines implémentations actuelles de blockchain ne peuvent traiter que quelques transactions par seconde, ce qui pourrait constituer un goulot d'étranglement potentiel pour l'IdO. Par rapport à l'évolutivité, la Blockchain peut avoir des blocages à cause de sa charge importante de transaction. Le stockage bitcoin par exemple est plus de 197 Go de stockage avec l'intégration de IoT à la blockchain

cela augmentera la charge ce qui constituera un obstacle car les objets connectés s'accroient de plus en plus. Par rapport à l'Interopérabilité, la blockchain peut être publique ou privée. Ainsi, l'interopérabilité entre les blockchains publiques et privées constitue également un défi dans l'approche Blockchain-IoT.

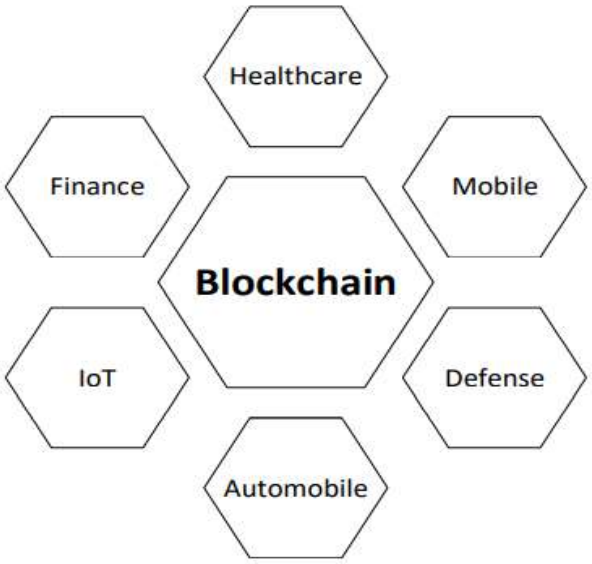


Figure 12: Domaine d'application de la blockchain

4.11 Conclusion

La blockchain est une technologie conçue de base pour le domaine de la cryptomonnaie ; mais de façon très rapide, elle a su se démocratiser et offre de nombreux avantages dans de beaucoup de domaines. Plusieurs chercheurs s'intéressent de plus en plus à la combinaison des technologies IoT et Blockchain notamment dans le domaine de la sécurité. Ils essaient de donner des solutions en se basant sur la méthodologie de la blockchain. De par sa nature décentralisée, elle vient apporter des solutions par exemple par rapport à l'écosystème IoT centralisé. Dans le chapitre qui suit, nous allons présenter des méthodes d'authentification basée sur la blockchain à travers des tableaux selon des critères mais aussi présenter deux de ces méthodes pour comprendre leur fonctionnement.

Chapitre 5 : Méthodes d'authentification basées sur la blockchain dans l'IoT

5.1 Introduction

Des recherches actives sont menées pour apporter des solutions d'authentification basées sur la blockchain pour les dispositifs IoT. Ces recherches s'appuient sur les caractéristiques de la blockchain tels que la décentralisation, les consensus pour la validation d'informations ou encore la distribution des copies du grand livre. Cependant les mécanismes proposés doivent tenir compte des caractéristiques de l'internet des objets qui sont souvent dures à combiner avec la blockchain mais aussi proposer des solutions pour faire face aux attaques existantes. Dans ce chapitre, nous allons présenter certaines méthodes d'authentification et présenter deux de ces méthodes d'authentification de façon détaillées.

5.2 Comparaison de différents Méthodes d'authentification

L'authentification entre les nœuds est essentielle au fonctionnement de la majorité des cas d'utilisation de l'IdO.

Nous avons passé en revue un bon nombre d'articles qui proposent des méthodes d'authentification basées sur la blockchain dans les environnements IoT. Les tableaux suivants décrivent de manière brève ces méthodes en s'accentuant sur des caractéristiques comme la résistance sur quelques types d'attaque liées à l'authentification, sur l'authentification mutuelle et l'intégrité qui sont aussi des exigences sécuritaires à satisfaire dans les systèmes IoT.

Tableau 1: Tableau comparatif de méthodes d'authentification

	Exemples de méthodes d'authentification basée sur la blockchain pour l'IoT				
Caractéristiques	[36]	[37]	[38]	[39]	[40]
Spécificité	Utilisation d'une chaine de hachage à sens unique pour l'authentifica-tion	Créer des bulles de confiance virtuelles	Proposer un système d'authentifica-tion web décentralisé	Proposer un système d'authentific ation pour les réseaux de capteurs WSN	Utilisation des Nœuds de brouillard pour permettre aux dispositifs d'être allégé de certaines tâches lourdes
Mesure en termes de performance	Réduit la charge de calcul ainsi que la latence	Réduit la consomma-tion d'énergie et de calcul	Création de compte utilisateur assez lente	Réduit la consomma-tion d'énergie et de calcul	Permet d'éviter la congestion, réduit la charge de calcul et la latence
Type de blockchain	Blockchain publique Ethereum	Blockchain publique Ethereum	Blockchain publique Ethereum	Blockchain privée Hyperledger-ger Fabric	Blockchain publique Ethereum
Authentification mutuelle	oui	oui	non	Pas Spécifié	oui
Intégrité	oui	oui	oui	oui	oui
Hétérogénéité	oui	oui	oui	non	oui
Scalabilité	oui	oui	oui	oui	oui

Le tableau ci-dessus compare différents types de méthodes d'authentification selon des critères. Chaque méthode possède une spécificité qui lui est propre pour pouvoir authentifier les dispositifs. Des mesures en termes de performance sont aussi indiquées dans le tableau ainsi que le type de blockchain utilisé. Nous avons aussi indiqué si les méthodes répondaient à certaines caractéristiques des systèmes IoT à satisfaire tels que l'authentification, l'intégrité mais aussi l'hétérogénéité des méthodes.

Tableau 2: Tableau comparatif des méthodes d'authentification par rapport à des attaques.

	[36]	[37]	[38]	[39]	[40]
Résistance à l'attaque par rejeu	oui	oui	oui	non	oui
Résistance aux attaques Man in the Middle	oui	non	non	oui	oui
Résistance aux attaques DoS	oui	oui	oui	oui	oui
Résistance aux attaques Sybil	non	oui	non	non	oui
Résistance aux attaques contre l'usurpation d'identité	non	oui	oui	non	oui

Ce tableau ci-dessus compare les différentes méthodes d'authentification selon des types d'attaques et indique s'ils sont résistants par rapport aux attaques.

Ces tableaux montrent les points forts et faibles des différentes méthodes. Ce qui nous a incités à faire une étude plus détaillée de deux mécanismes d'authentification qui remplissent plusieurs critères. Ces méthodes sont celles proposées dans l'article [37] et [40].

5.3 Études de méthodes d'authentification basées sur la blockchain pour l'IoT

5.3.1 Protocole d'authentification pour l'IdO

Présentation du protocole :

Le protocole d'authentification proposé permet une authentification des dispositifs en se basant sur la blockchain et les nœuds de brouillard. Il utilise des certificats basés sur la cryptographie à courbe elliptique (ECC). Les dispositifs IoT dans ce contexte sont limités en termes de capacité de stockage et de traitement [40].

Architecture proposée :

L'architecture, selon l'auteur, se compose de ces différents acteurs, dispositifs IoT, passerelles ou nœuds de brouillard, contrôleurs, de serveur en nuage, de contrat intelligent et de la blockchain (voir figure 13).

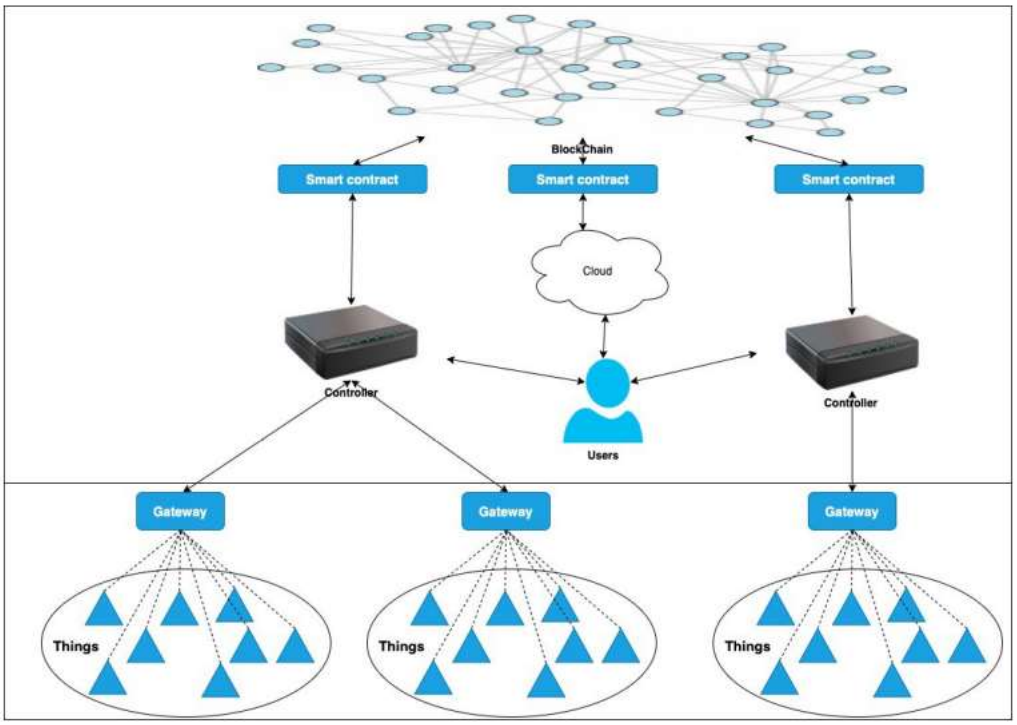


Figure 13: Architecture du protocole d'authentification pour l'IdO utilisant la blockchain et le fog computing [40]

Ces différents participants ont chacun un rôle dans le processus :

- Utilisateurs : les utilisateurs ou encore clients du système ont pour rôle de s'enregistrer sur le formulaire d'inscription du serveur en nuage et ensuite enregistrer leurs dispositifs IoT sur ce serveur.
- Dispositifs IoT : Ces dispositifs enregistrés sur le serveur permettent d'obtenir des clés privées
- Passerelles : une passerelle ou nœud de brouillard est capable de gérer plusieurs dispositifs et est gérée à son tour par un contrôleur. Les passerelles gèrent le traitement lourd que les dispositifs ne peuvent pas assurer.
- Contrôleurs : Ils assurent l'enregistrement ainsi que la gestion des passerelles vers la blockchain.
- Serveur de nuage : Dans cette approche, il n'existe qu'un seul serveur cloud. Ce serveur est responsable du déploiement du contrat intelligent lors de la création d'un utilisateur, de l'ajout de dispositifs, de la génération des clés privés ou encore de l'enregistrement du contrôleur dans la blockchain.
- Contrat intelligent : Seul un contrat intelligent est généré dans ce protocole proposé. Il permet d'ajouter des utilisateurs, des passerelles, des dispositifs et des utilisateurs. Il authentifie les demandes et ajoute une certaine logique commerciale dans la blockchain.

Les différentes phases du protocole :

- Phase d'enregistrement des utilisateurs
  L'enregistrement des utilisateurs est la première étape à assurer, l'utilisateur enregistre ses données ou informations dans un formulaire d'enregistrement situé au niveau du serveur cloud. Le serveur va, par la suite, envoyer ces données à la fonction du contrat intelligent l'addUser. Seul ce serveur est capable et autorisé à appeler cette fonction du contrat intelligent.

- Phase d'enregistrement des dispositifs

  L'enregistrement des dispositifs IoT de l'utilisateur se déroule en 2 étapes :

  La première étape : l'utilisateur enregistre ses appareils au niveau du formulaire du serveur cloud. Ce dernier va ajouter le nœud à la blockchain avec la fonction Add device du contrat intelligent. Après cette étape l'utilisateur va obtenir une clé privée pour pouvoir configurer le dispositif qui va ensuite pouvoir générer une clé publique ECC à partir de cette clé privée.

  La deuxième étape consiste à l'envoi d'une demande d'enregistrement des dispositifs au niveau de la passerelle. Cette demande contiendra la clé publique du dispositif. La passerelle va répondre à cette demande avec sa clé publique. Par la suite, son identifiant est pré-intégré avec des informations et un nonce chiffré avec la clé publique de la passerelle.

  Un TimeStamp sera intégré à la requête du dispositif pour permettre à la passerelle de contrôler si la demande est récente ou pas. Ensuite la passerelle va valider en interne et envoyer une demande d'enregistrement du dispositif au niveau du contrôleur en y intégrant les informations précédemment évoquées lors de l'enregistrement du dispositif au niveau de la passerelle mais avec cette fois-ci une deuxième différente de celui du premier dans le message.

- Phase d'authentification

  Le contrôleur va recevoir la demande d'enregistrement du dispositif chiffrée et va vérifier l'identité du dispositif au niveau de la blockchain. S'il existe au niveau de la blockchain le contrôleur va ajouter la clé publique et les autres informations du dispositif en utilisant le contrat intelligent.

5.3.2 Mécanisme d'authentification Bubbles of Trust

Présentation du mécanisme d'authentification [37] :

Le mécanisme proposé dans cette partie est un système d'authentification décentralisé efficace basé sur la blockchain plus particulièrement celle de la blockchain publique Ethereum. Dans cette approche des zones virtuelles sécurisées sont créées dans les environnements IoT où les dispositifs ne peuvent communiquer qu'avec des dispositifs qui se trouvent dans la même zone ainsi

tout dispositif ou appareil ne se trouvant pas dans la zone est considéré comme malveillant. Le fait que des dispositifs de même zone communiquent de manière sécurisée installe une certaine confiance entre les dispositifs d'où le nom de bulle de confiance. Cette bulle est protégée et inaccessible aux autres dispositifs.

Fonctionnement du système

Le fonctionnement du système est expliqué sur différentes phases :

- La première phase montre que les dispositifs IoT peuvent être de nature différentes et de domaines différents (médical, industriel, environnement, etc.).
- La deuxième phase ou phase B correspond à la phase d'initialisation. L'approche proposée ne nécessite pas de matériel spécial pour mettre en œuvre celle-ci ; il est par contre primordial de démarrer par une phase d'initialisation. Dans cette phase, un maitre de bulle est désigné, il faut noter cependant que ce maitre de bulle peut être n'importe lequel des dispositifs. Il peut être considéré comme étant une autorité de certification et possède une paire de clé (privée/publique). Même en étant hors service, le maitre d'une bulle ne perturbe pas le fonctionnement de celle-ci.

  Tous les autres nœuds des zones sont appelés suiveurs. Chaque suiveur génère une paire de clé privée/publique à courbe elliptique (ECC). Chaque suiveur dans ce schéma aura en sa possession un ticket (signé par le maitre de bulle) qui est le certificat (voir figure 14). Les certificats sont légers (64 octets) et contiennent les informations suivantes :
  - Un groupID (grpID) qui est le numéro de la bulle dont le suiveur fera partie ;
  - Un objectID (objID) qui est l'identifiant du suiveur dans la bulle ;
  - Un pubAddr qui est l'adresse publique du suiveur. Elle représente les 20 premiers octets de hachage Keccak (SHA-3) de la clé publique du suiveur ;
  - Une structure de signature qui est la signature de l'algorithme de signature numérique à courbe elliptique (ECDSA) utilisant la clé privée du maitre de bulle

```
==========================================
GroupID : XX
ObjectID   :
YY PubAddr :
@@
==========================================
Signature (keccakhash(XX||YY||@@))
==========================================
```

Figure 14: Structure d'un ticket dans Bubbles of trust [37]

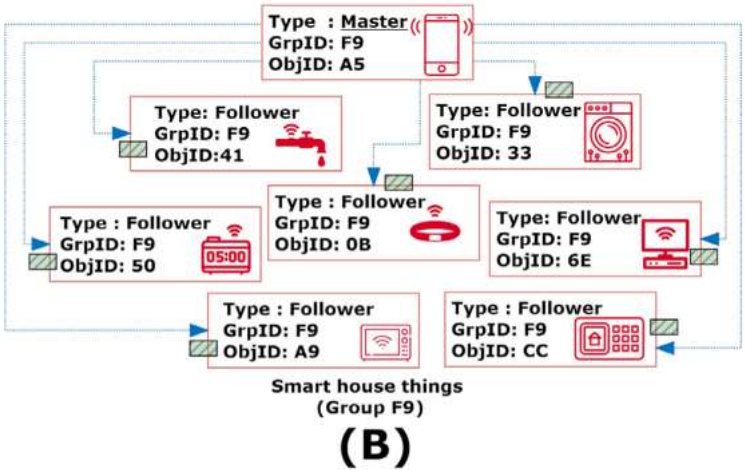


Figure 15: phase d'initialisations dans Bubbles of trust [37]

- La troisième phase qui correspond à la phase C qui consiste à créer les bulles de confiance dans la blockchain. Pour cela le maitre d'une bulle envoie une transaction contenant l'identifiant du maitre et l'identifiant du groupe qu'il veut créer. Ensuite la blockchain vérifie si ces informations sont uniques. Si cette transaction est validée par la blockchain, la nouvelle bulle est ainsi créée.

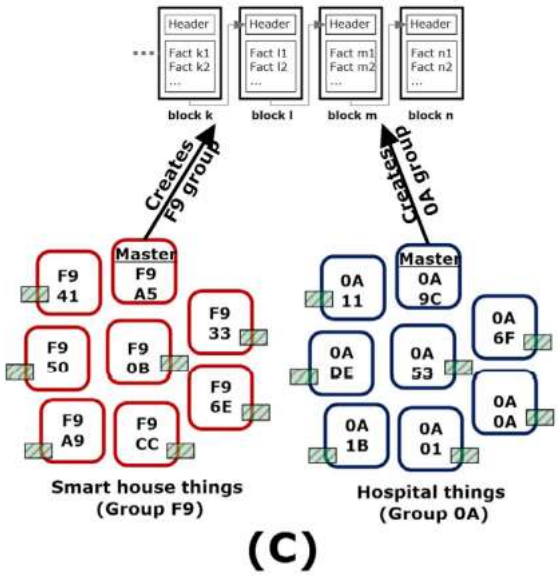


Figure 16: Phase de création de bulles de confiance [37]

- Suite à la création des bulles, les suiveurs (followers) seront en mesure d'envoyer à leur tour des transactions à la blockchain pour être associés à leurs bulles respectives dans la phase (D). Le contrat intelligent permet de vérifier l'unicité de l'identifiant du suiveur et celle de l'identifiant de la bulle. Il vérifie ensuite la validité du ticket avec la clé publique du maitre. Une fois la première transaction (demande d'association) d'un suiveur est réussie, ce dernier n'a plus besoin d'utiliser son ticket pour s'authentifier (il l'envoie au sein des messages échangés).

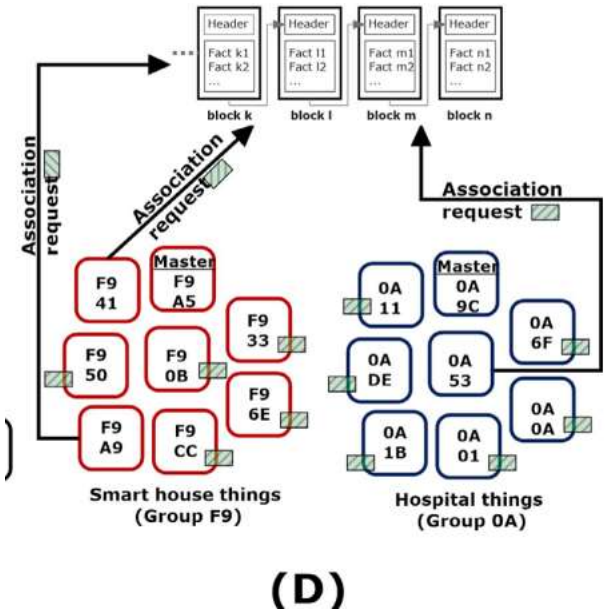


Figure 17: Demande d'association [37]

- La demande d'association du suiveur dans la blockchain correspond à la première transaction effectuée par le suiveur dans la blockchain. La transaction contient le ticket du suiveur signé avec la clé privée de celui-ci. Le ticket se compose comme nous l'avons souligné tout à l'heure de l'identifiant de la bulle ou XX sur le schéma ci-dessous, de l'identifiant du suiveur ou YY et de la clé publique du suiveur PubKey_F. La clé publique contenue dans le ticket permet de pouvoir de vérifier l'intégrité du message. Le ticket du suiveur sera ensuite vérifié avec la clé publique du maitre. Si toutes les informations sont valides alors les paramètres seront stockés dans la blockchain.

- Phase d'authentification du suiveur

  Lorsque ce suiveur envoie dans un autre temps une transaction, celle-ci contiendra les données échangées : XX, YY et la signature ECDSA de sa concaténation des champs précédents à l'aide de la clé privée du suiveur. La blockchain, après avoir reçu la transaction, vérifie l'intégrité avec la clé publique du suiveur si la signature est valide, elle vérifie par la suite la clé publique utilisée pour la vérification de la transaction si elle est stockée et associée aux grpID et objID envoyés dans la transaction, si l'association est bien stockée et valide alors la phase d'authentification du dispositif est réussie (voir figure 18).

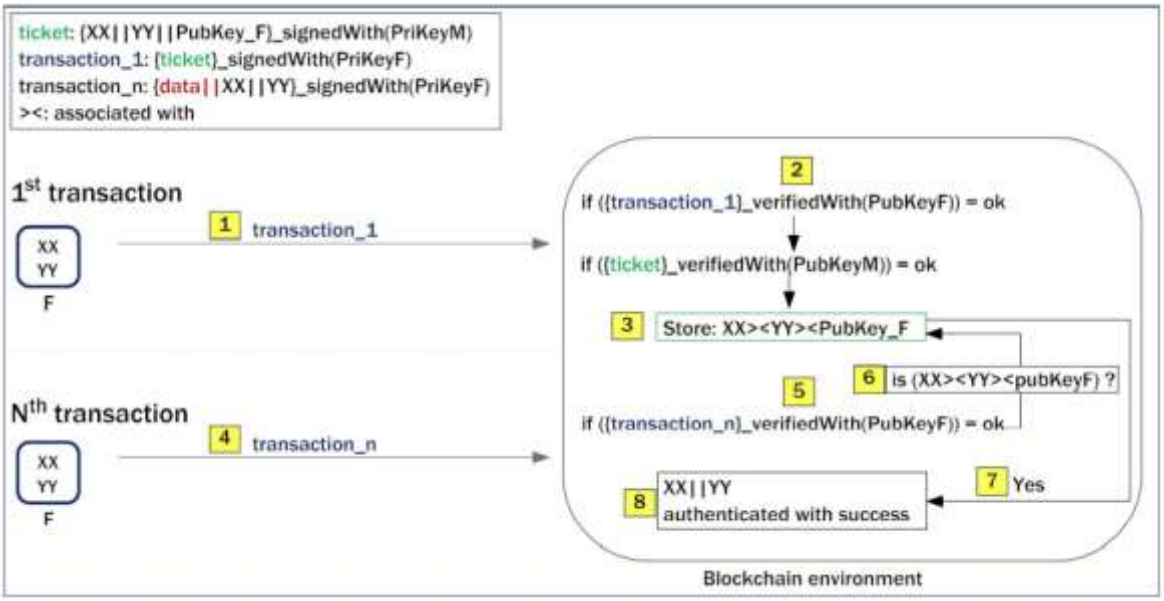


Figure 18: Authentification d'un suiveur dans la blockchain [37]

5.4 Conclusion

Dans ce chapitre nous avons étudié un ensemble de mécanismes d'authentification basées sur la blockchain pour les objets connectés et faire leur analyse par rapport aux attaques et sur d'autres critères de sécurité. Ensuite nous avons présenté deux de ces mécanismes et nous avons décrit leur fonctionnement. Les protocoles décrits dans ce chapitre prouvent leur légèreté et leur robustesse cependant ils ne garantissent pas une bonne sécurité. En effet ils ne sont pas résistants à toutes les attaques qui peuvent exister. Il faut noter aussi que l'intégration de la technologie Blockchain dans un système IoT présente des limites. C'est dans ce contexte que nous avons proposé un nouveau protocole d'authentification qui va s'inspiré de la technologie blockchain pour pouvoir apporter des solutions par rapport à la limite de cette intégration et garantir que l'environnement IoT sera résistant à certains attaques. Dans le chapitre suivant nous allons présenter ce nouveau protocole de façon plus détaillée.

Chapitre 6 : Proposition d'un nouveau protocole d'authentification inspirée de la blockchain dans l'IoT.

6.1 Introduction

La plupart des méthodes existantes concernant l'authentification décentralisée des nœuds IoT se basent sur la technologie blockchain. Cependant cette technologie présente des limites qu'il faut bien tenir en compte. Le stockage bitcoin par exemple est plus de 197 Go, avec l'intégration de l'IoT à la blockchain. Cela a pour effet d'augmenter la charge, ce qui constitue un obstacle car les objets connectés sont d'une part très limités en ressources, et d'autre part, leur nombre s'accroît de manière exponentielle. Pour apporter des solutions à ces différents problèmes nous avons proposé un nouveau protocole qui va s'inspirer de la blockchain et permettre de garantir une sécurité au sein d'un environnement IoT.

6.2 Approche :

Comme contribution par rapport à notre mémoire, nous avons essayé de proposer un nouveau protocole d'authentification des objets IoT en se basant sur certaines caractéristiques de la blockchain. Notre objectif principal est de proposer un mécanisme permettant à des nœuds IoT voisins d'un réseau de s'authentifier de façon décentralisée et échanger des informations qui sont secrètes de façon sécurisée. Comme dans la blockchain notre approche va garantir une confiance entre les différents nœuds du réseau.

Notre solution décentralisée se caractérise par un mécanisme de distribution de blocs de secrets détenus par les différents nœuds. Ceci va permettre aux différents nœuds d'authentifier les nouveaux objets désirant intégrer le réseau. Cette solution repose sur l'utilisation de la cryptographie asymétrique (paires des clés publiques/privées).

De plus, comme nous le verrons ici, notre protocole comporte deux versions dont une qui permet d'offrir une fonctionnalité d'authentification légère avec un très haut de sécurité garanti.

6.3 Schéma :

Notre concept se caractérise principalement d'un serveur contenu dans le cloud qui contient notamment un ensemble de blocs dit 'secrets' car contenant des informations qui ne sont accessibles qu'aux objets autorisés.

- Le serveur

  Dans ce nouveau concept, nous avons mis en place un serveur qui va permettre de stocker et de distribuer des blocs de secrets et qui va permettre plus tard aux nœuds de s'authentifier. Le serveur ne va pas s'impliquer dans la démarche d'authentification des nœuds mais va plutôt être comparée à une base de données. Ce serveur dans le cloud va permettre l'initialisation des nœuds et leur première intégration dans le réseau. Il va contenir d'autres informations telles que les empreintes ou hash des différents blocs de secrets, de ceux des nœuds mais aussi d'autres informations utiles pour un administrateur comme un système d'horodatage qui permet d'avoir des renseignements sur la date de distribution d'un bloc à un nœud où de sa création et un autre système de comptage qui va permettre de relier l'identifiant d'un nœud à un bloc. En outre, ce serveur devra stocker les clés publiques des nœuds auxquels il va affecter des blocs. Notre serveur possède sa propre clé publique qui lui permet de pouvoir distribuer les blocs de secrets aux différents nœuds. Dans notre solution nous avons proposée deux solutions d'authentification, une version légère et une version lourde. Dans la version lourde le serveur va chiffrée le message secret contenu dans le bloc avec une clé secrète qui sera distribuée aux nœuds.

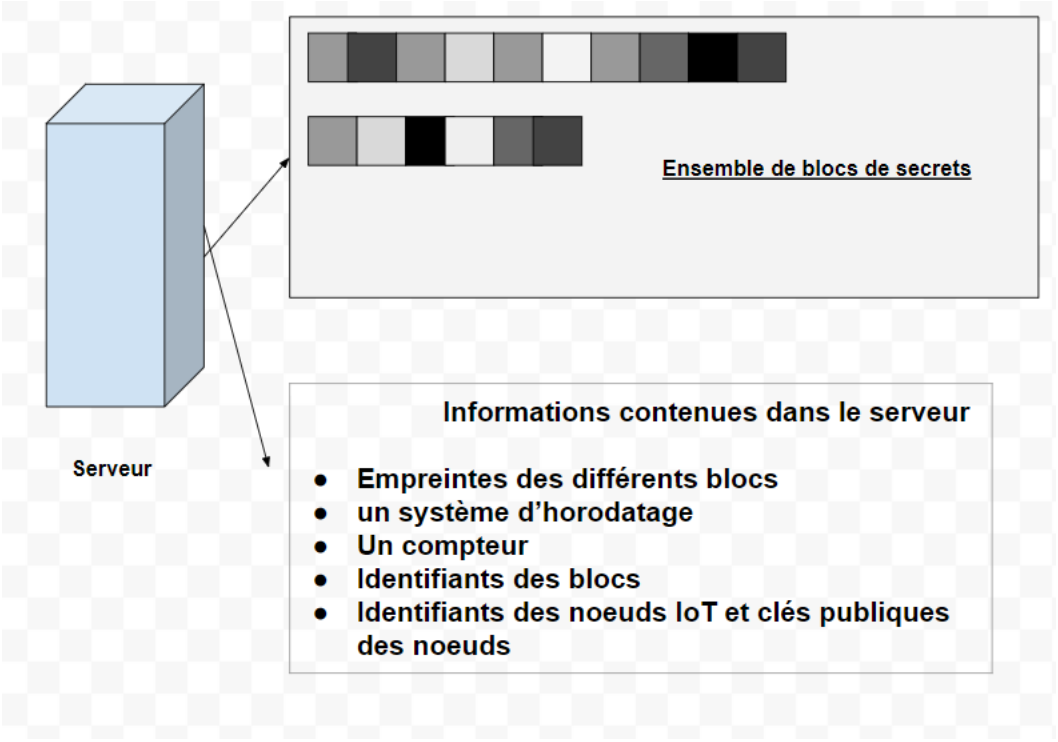


Figure 19:Serveur pour la gestion et la distribution de blocs de secrets

❖ Les blocs de secrets

Le concepteur des blocs de secrets va créer à partir d'un secret une empreinte ou un hash grâce à l'utilisation d'une fonction ou algorithme de hachage. Cet algorithme permet de prendre un message donné et de générer un condensé appelé hash. Il permet d'assurer l'intégrité d'un message et son authenticité. Dans notre approche, l'utilisation de cet algorithme pour générer un hash va permettre à des nœuds qui ont des blocs en commun de pouvoir s'authentifier de deux manières différentes :

- Ainsi, dans la version légère du protocole, les nœuds vont se baser uniquement sur les empreintes de leurs blocs pour pouvoir valider une authentification.
- En revanche, dans la version lourde du protocole, en plus des empreintes de leurs blocs, les nœuds vont aussi vérifier le message secret avec la clé secrète distribuée lors de la phase d'initialisation afin de valider une authentification.

Pour le hachage du message qui doit être un secret nous avons opté pour des fonctions de hachage de 128 bits qui sont légères en termes de stockage.

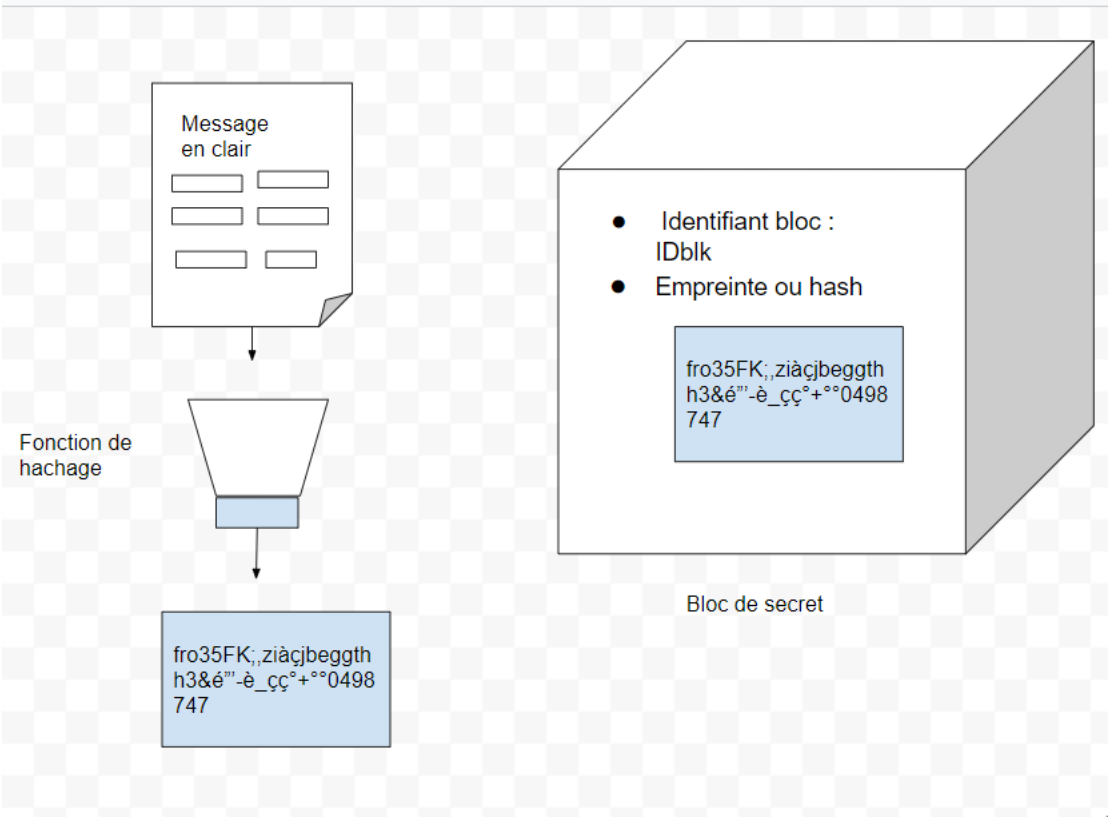


Figure 20:Structure d'un bloc secret

6.4 Phase d'initialisation

Notre approche débute d'abord par une phase d'initialisation des différents nœuds qui vont constituer notre réseau. C'est là où intervient le serveur situé dans le Cloud. Cette phase d'initialisation est commune aux deux versions légère et lourde du protocole. Les différents blocs de secrets créés dans le serveur vont être distribués aux différents nœuds du réseau.

La phase d'initialisation peut être résumée comme suit :

1. Un nœud demande la clé publique serveur avec une requête.
2. Le serveur envoie sa clé publique au nœud.
3. Le nœud va ensuite envoyer un message chiffré avec la clé publique du serveur contenant son identifiant et sa clé publique.
4. Le serveur stocke ses informations
5. Le serveur distribue des blocs de secret au nœud.

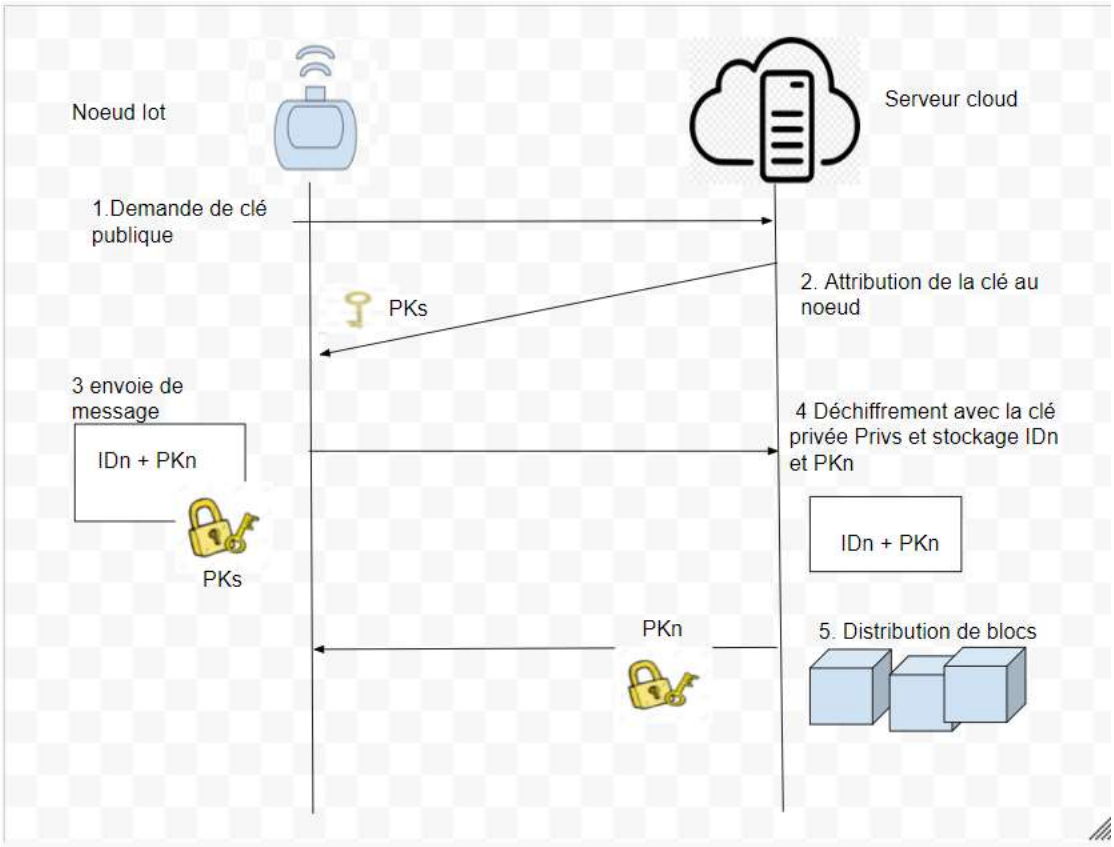


Figure 21:Schéma de la phase d'initialisation du réseau

1. Attribution des blocs secrets

Un nœud qui arrive dans le réseau se fera attribuer un ou plusieurs blocs. L'attribution des blocs dépendra d'un paramètre : l'empreinte du bloc qui va permettre au concepteur du réseau d'associer le nœud à un ou plusieurs blocs selon des paramètres qu'il va développer. Le nœud va d'abord envoyer une requête au niveau du serveur pour lui demander sa clé publique. Ce nœud va ensuite envoyer un message d'enregistrement contenant son identifiant et sa clé publique chiffrée avec la clé publique du serveur. La clé publique du nœud va par la suite être stockée dans le serveur ainsi que son identifiant. Ensuite le serveur va envoyer les blocs de secret aux nœuds à travers un message chiffré avec la clé publique du nœud.

Il faut noter ainsi, que dans le réseau, plusieurs nœuds peuvent avoir en commun un ensemble de blocs de secrets.

Lorsque qu'un nœud se fera distribuer des blocs, il va stocker les empreintes des blocs de secret des différents blocs. Nous avons estimé que le nombre de blocs que l'on peut attribuer ne doit pas dépasser un certain seuil car les objets IoT

ont tendance à avoir une faible capacité de stockage de ce fait nous avons limité le nombre de stockage de bloc à un nombre alpha car les objets auront un nombre important de bits notamment les identifiants des nœuds et de leur clé de chiffrement.

Au niveau du serveur lorsqu'un nœud se fera attribué des blocs, ils seront horodatés c'est-à-dire que l'identifiant du nœud sera associé à celui du bloc ou des blocs ainsi que le moment de l'association. Mais aussi le compteur décompte le nœud comme étant le premier à être associé à un nœud ainsi de suite et va l'associer avec son identifiant.

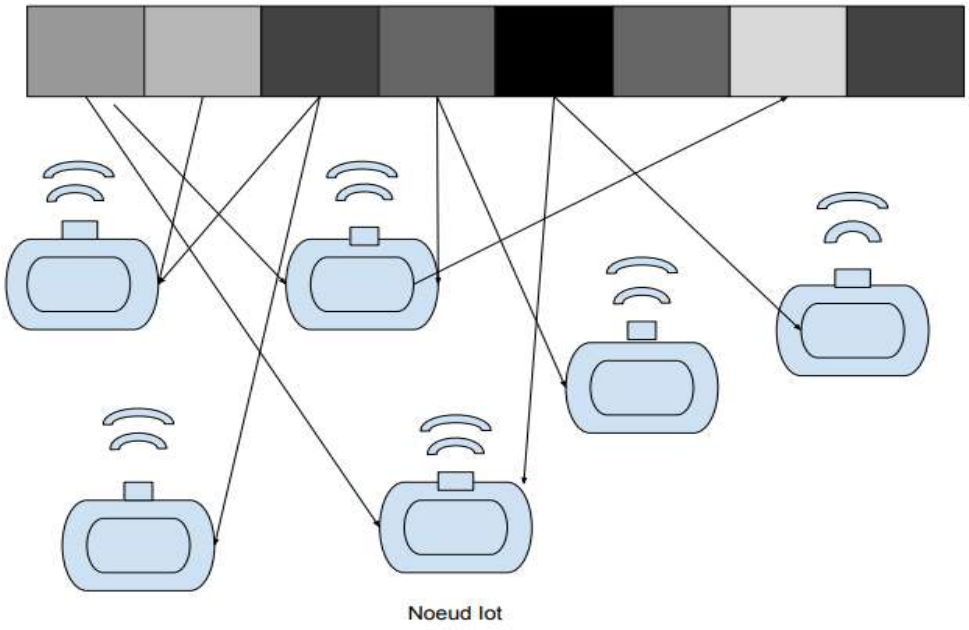


Figure 22: Distribution de blocs de secrets aux différents nœuds IoT

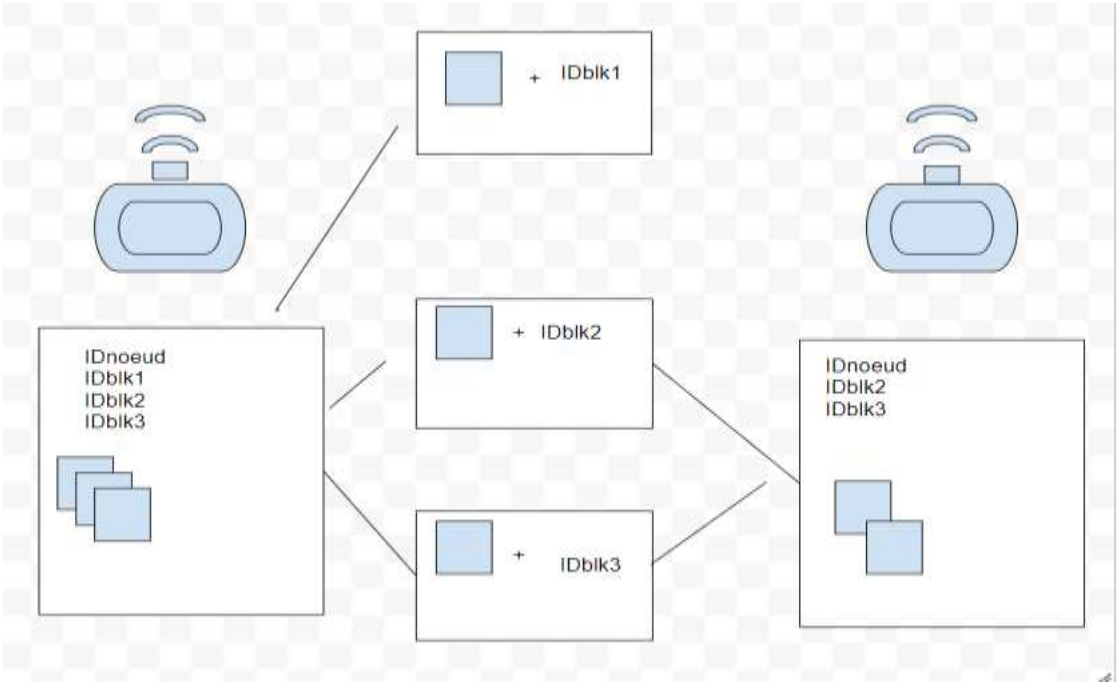


Figure 23: Exemple d'attribution de blocs de secrets à des nœuds IoT différents

2. Génération de clés publiques

A chaque attribution de blocs de secret les nœuds vont générer une paire de clé privée/publique pour permettre de chiffrer et déchiffrer les messages qu'ils vont s'envoyer dans le réseau notamment pour l'authentification. L'ajout de clés chiffrement dans notre réseau va permettre d'augmenter la sécurité dans le réseau. Les nœuds étant parfois très limité en terme stockage comme nous l'avons évoqué plus haut, nous avons opté pour des clés publiques à courbes elliptiques car étant des clés de plus petites tailles et plus rapides.

6.5 Phase d'authentification

Notre approche vise essentiellement à créer un réseau de nœuds qui vont pouvoir s'authentifier mutuellement pour garantir une certaine sécurité et ne pas permettre à des malveillants de s'introduire, d'avoir accès aux secrets détenus dans le réseau ou même de communiquer avec les autres nœuds du réseau. La première phase d'initialisation aura permis de mettre en place un système pour distribuer les blocs. La deuxième et la plus importante concerne l'authentification des nœuds auprès des autres nœuds.

1. Demande de clés publiques

   Après avoir effectué l'initialisation des nœuds dans le réseau nous avons voulu garantir une confiance entre les nœuds du réseau. Pour cela un nœud par exemple va demander les clés publiques de ses voisins qui vont l'authentifier. Le nœud en question aura besoin de ces clés pour chiffrer un message et l'envoyer aux nœuds voisins pour s'authentifier. Pour obtenir les clés publiques, le nœud va envoyer par diffusion une requête pour demander aux nœuds voisins de lui envoyer leurs clés. Les voisins du nœud sont les nœuds IoT qui sont plus proches en termes de distance Chaque nœud voisin va ensuite envoyer sa clé par message unicast.

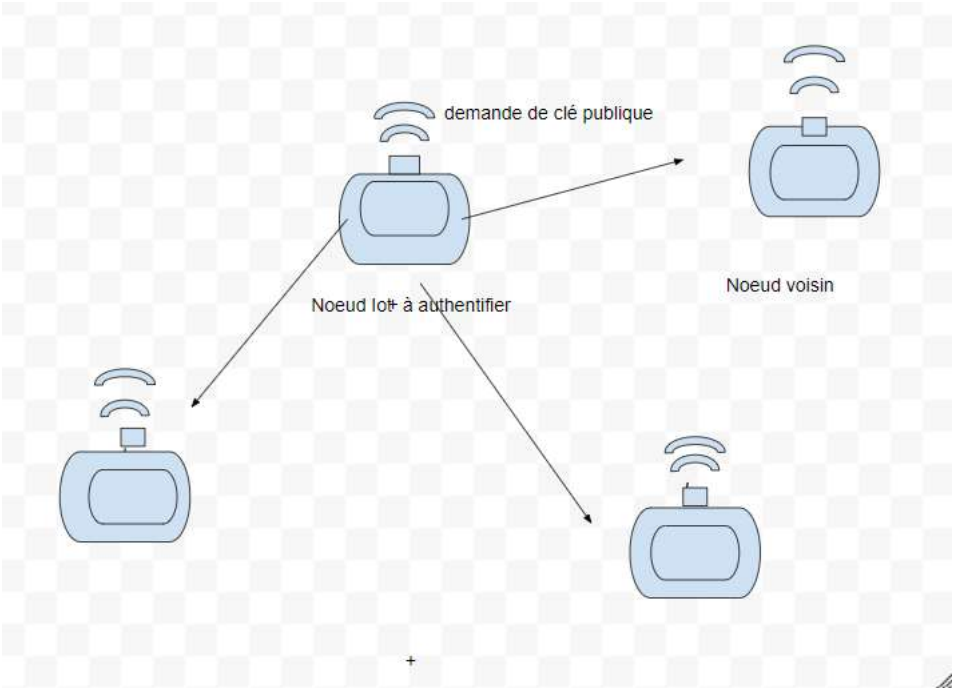


Figure 24:demande de clés publiques aux noeuds voisins

2. Diffusion de message crypté

   Le nœud va chiffrer à partir de ces clés publiques un message pour son authentification. Ce message contiendra son identifiant, l'identifiant du bloc ou les identifiants de blocs de secrets qu'il possède avec leurs empreintes mais aussi un hash ou empreinte pour garantir aux voisins que ce message provient bien de ce nœud. L'empreinte est l'élément essentiel pour authentifier un nœud. Le hash permet de pouvoir conserver les informations c'est-à-dire de pouvoir garantir l'intégrité et l'authenticité du message. Le hash est accompagné de la clé publique du nœud qui va permettre au nœud de calculer la fonction de hachage.

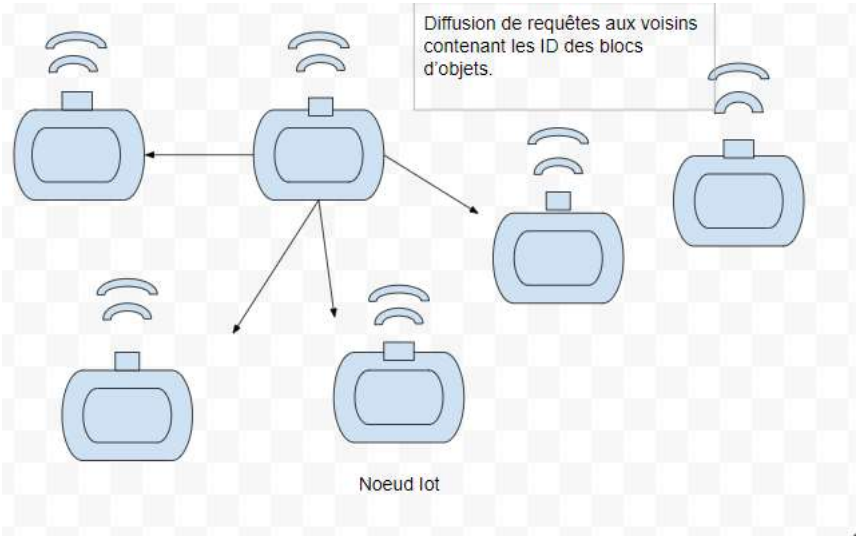


Figure 25:Demande d'authentification auprès des voisins

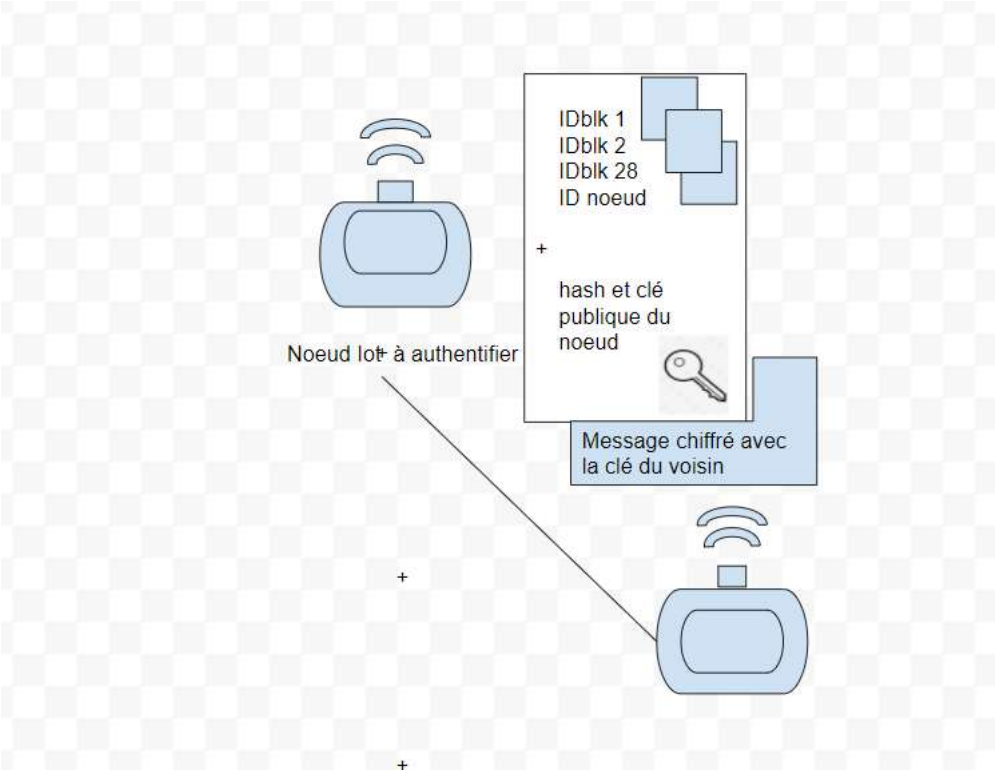


Figure 26:Demande d'authentification auprès d'un voisin

3. Vérification de l'information envoyée aux voisins

Les différents nœuds voisins vont déchiffrer le message reçu avec leurs propres clés privées premièrement et vont ensuite devoir calculer la fonction de hachage pour vérifier si le message n'a pas été modifié par un attaquant à l'aide de la clé publique du nœud. Si ces informations sont correctes, les nœuds voisins vont ensuite voir s'ils possèdent un ou plusieurs empreintes de blocs correspondants aux empreintes qu'ils détiennent dans leurs trousseaux.

De ce fait, si un nœud voisin reconnait un ou plusieurs empreintes, il va envoyer une notification avec la clé publique du nœud déjà envoyée pour indiquer au nœud qu'il reconnait son bloc ou ses blocs.

Dans la version légère du protocole, le processus d'authentification s'arrête à cette étape dès lors que le taux d'acceptation est satisfait. Tandis que, dans sa version lourde, le processus d'authentification se poursuit avec d'autres étapes. Le nœud b s'il reconnait des empreintes dans son trousseau va par la suite déchiffrée le message contenu dans le bloc avec la clé secrète qu'il détient.

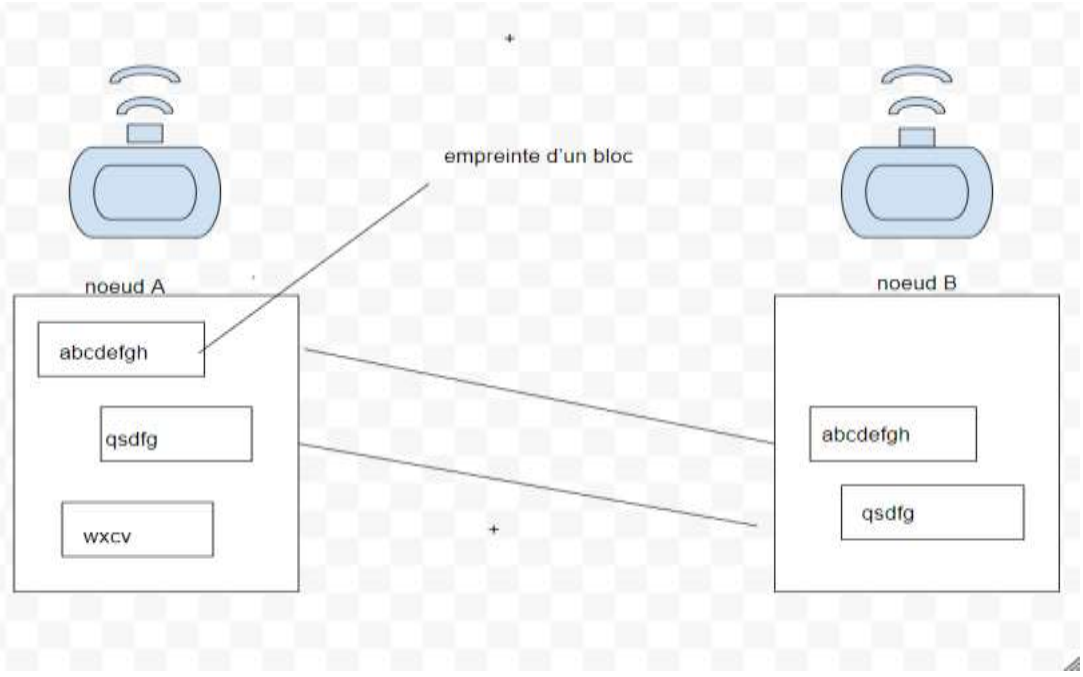


Figure 27: Vérification des blocs en commun

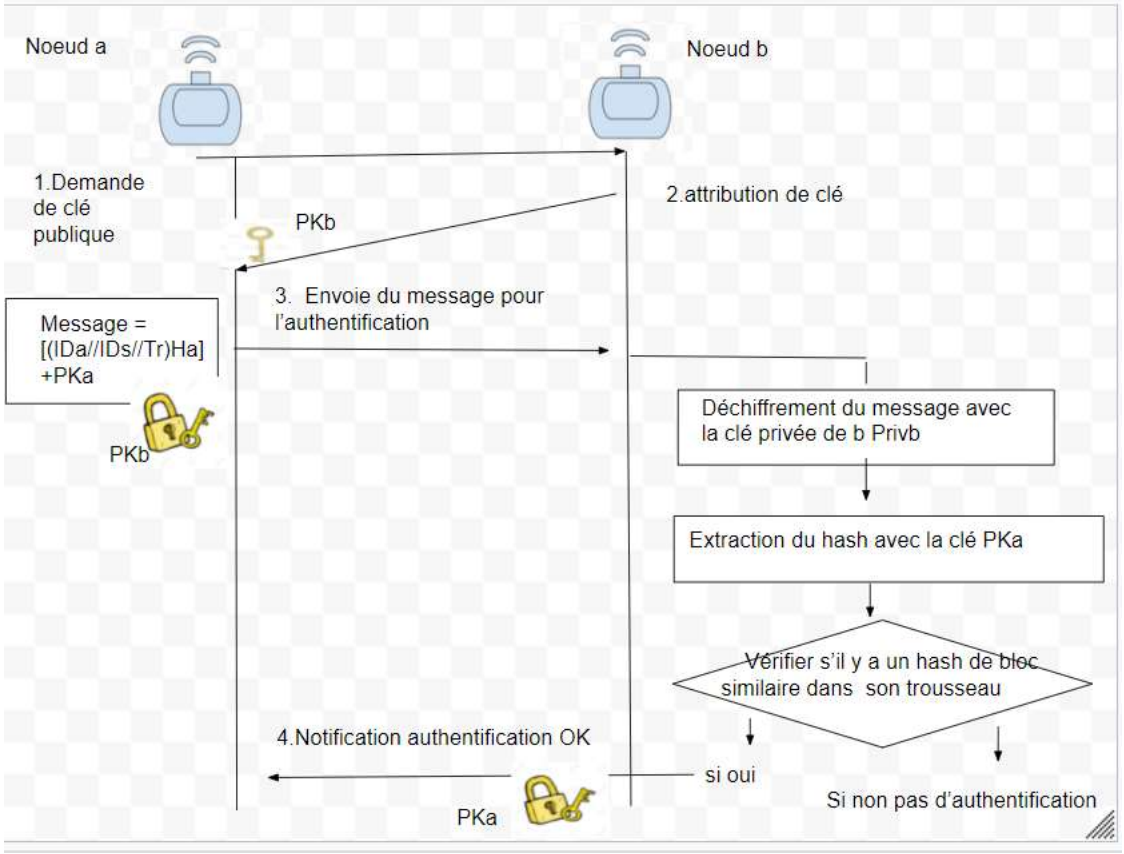


Figure 28:Schéma d'authentification de la version légère du protocole

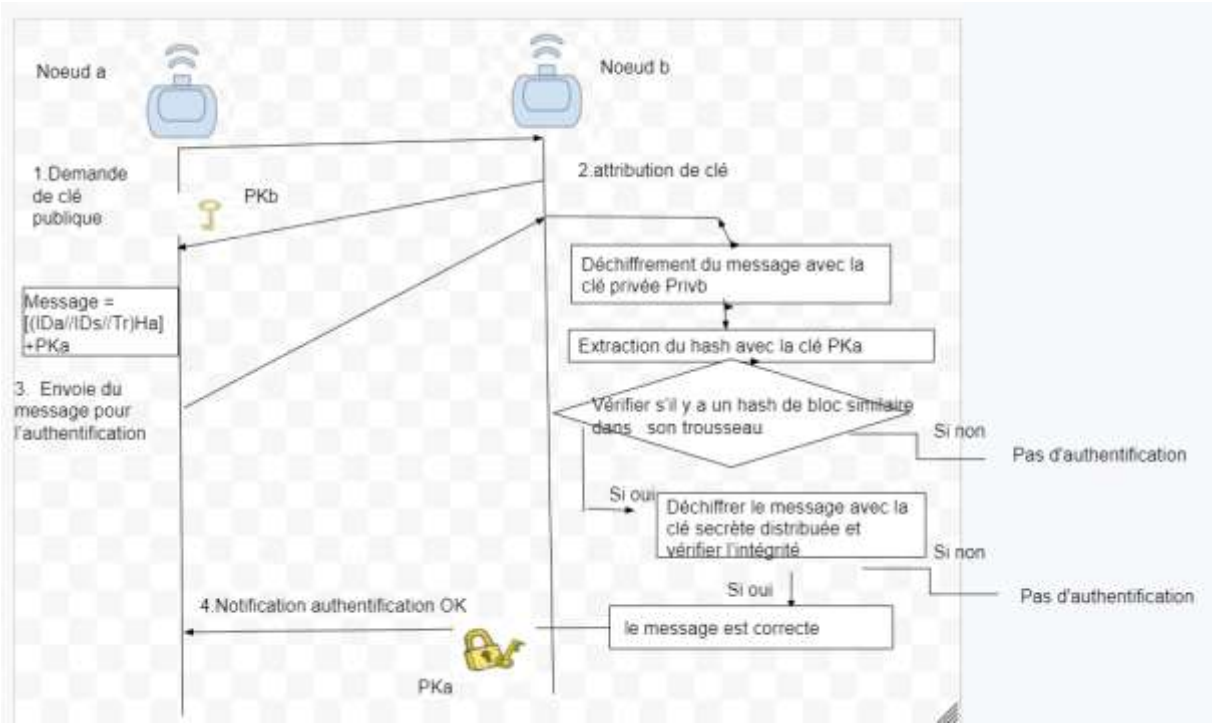


Figure 29:Schéma d'authentification de la version lourde du protocole

4. Authentification du nœud voisin
   Lorsque le nœud voisin a reconnu et vérifier les informations (hash et bloc de secret), il a donc pu authentifier le nœud à son tour il va s'authentifier auprès de ce nœud pour cela, il va envoyer à son tour en cryptant un message de confirmation avec la clé publique du nœud. Ce message de confirmation va contenir son identifiant ainsi que l'empreinte du bloc ou des blocs, sa clé publique et un hash.

5. Validation de l'authentification du nœud
   La phase d'authentification sera complète que lorsqu'un taux d'acceptation sera atteint c'est-à-dire qu'un bon nombre de nœuds possédant les blocs en commun avec le nœud auront confirmé avoir reconnu les empreintes des blocs de secrets. Donc le nœud doit valider un certain nombre d'authentification pour qu'il puisse être authentifié. Ce nombre lui permettra de pouvoir communiquer avec les autres nœuds authentifiés.
   Dans le cas où les nœuds voisins ne parviennent pas à reconnaitre les blocs de secret, ils vont relayer l'information au niveau de leurs voisins pour qu'ils vérifient à leur tour s'ils reconnaissent un ou plusieurs de ces blocs de ce trousseau. Et ce processus sera répéter jusqu'à ce que tous les voisins soient atteints.

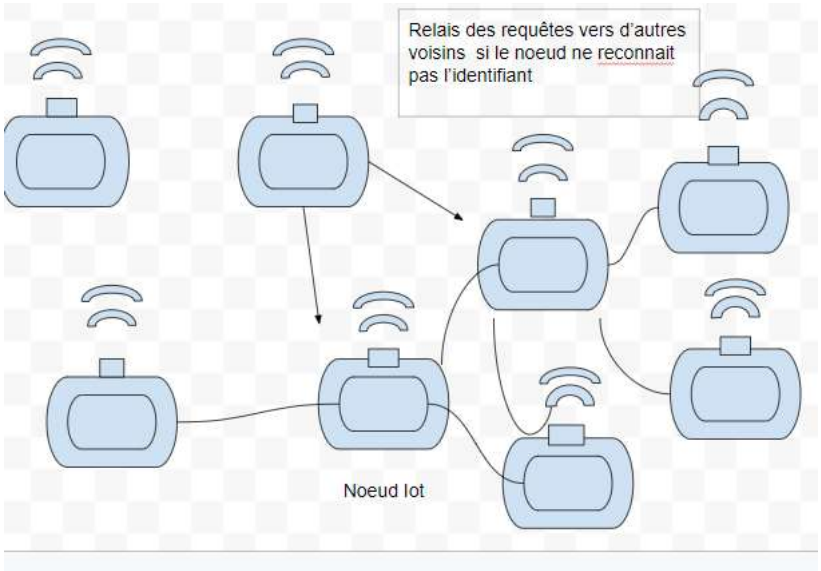


Figure 30:Relais de message aux autres voisins

Tableau 3:Paramètres du protocole

Paramètres	Descriptions
Ha	Hash du message venant de a
Ida	Identifiant du nœud a
IDn	Identifiant du nœud
IDs	Identifiants des blocs
PKa	Clé publique du nœud a
PKb	Clé publique du nœud b
PKn	Clé publique du nœud
PKs	Clé publique du serveur
Privb	Clé privée du nœud b
Privs	Clé privée du serveur
Tr	Trousseau d'empreintes de a

6.6 Phase de maintenance

Cette phase correspond à la gestion des clés cryptographiques utilisées par les différents nœuds du réseau. Un des paramètres de la gestion dans notre cas est la génération de clés. Les nœuds après leurs initialisations seront capables de générer de façon locale leurs clés publiques. Ces clés publiques auront une durée de vie pour ne pas surcharger les équipements IoT. Leur durée de vie commence lorsque de la phase de l'authentification doit commencer et se termine lorsque le nœud aura été authentifié par un bon nombre de nœuds. Après cette phase il est possible que le nœud révoque sa paire de clé pour s'authentifier dans le réseau s'il n'était plus présent dans le réseau pendant un certain moment.

6.7 Analyses du nouveau protocole proposé

- Analyse par rapport à la taxonomie des schémas d'authentification.

Tableau 4:Analyse du protocole par rapport è la taxonomie de schéma d'authentification

Critères :	Méthodes utilisées :
Facteur d'authentification	Authentification de l'identité
Authentification à base de jetons	Oui : les blocs de secrets peuvent être considérés comme les jetons
Procédure d'authentification	Authentification bidirectionnelle ou authentification mutuelle
Couche IoT	Perception
Authentification basé sur le matériel physique	Pas utilisée ici, mais possible si les blocs de secrets sont gravés de manière intrinsèquement liée au matériel
Architecture d'authentification	Décentralisation

- Analyse par rapport aux exigences d'authentification de l'IoT.

Tableau 5:Analyse par rapport aux exigences d'authentification

Exigences :	Etats :
Système léger	Oui : les clés cryptographique et fonctions de hachages de hachage sont centralisée
Authentification multifactorielle	Oui : Avec notamment l'utilisation des blocs de secrets comme facteurs mais aussi le taux de similarité de blocs de nœuds
Efficace	Oui
Technique de cryptographie	Utilisation de clé asymétrique de type ECC

❖ Analyse du protocole proposé par rapports aux attaques.

Tableau 6:Résistance du protocole proposé par rapport aux attaques

Types d'attaques	Résistance	
	Phase d'initialisation	Phase d'authentification
Insertion de nœuds malveillants	✓	✓
Attaque par force brute	✓	✓
Attaque DoS/DDoS	x	✓
Attaque Sybil	✓	✓
Attaque par usurpation d'identité	✓	✓
Man in the middle	✓	✓
Attaque par rejeu	✓	✓

❖ Analyse du protocole par rapport aux attaques.

- Insertion de nœud malveillant

  Lors de la phase d'authentification, il est possible que des nœuds malveillants demandent à être authentifié par les nœuds du réseau. Ces nœuds malicieux qui n'ont pas été initialisé par le serveur vont tenter de générer des empreintes pour pouvoir être authentifié et ces empreintes doivent correspondre aux empreintes contenues dans le trousseau des différents nœuds du réseau. Un nœud malveillant peut générer un bon nombre d'empreintes avant de pouvoir être enfin authentifié dans le réseau. Mathématiquement parlant la probabilité qu'un nœud puisse être authentifié doit dépendre d'un certain nombre de paramètres tels que : le nombre moyen de blocs qui existent dans le voisinage du nœud, la taille du hash (128, par exemple), de la densité du réseau mais aussi du taux d'acceptation.

  Dans un premier temps la probabilité pour qu'un nœud malicieux trouve une empreinte correspondante à un nœud légitime est égale au nombre de blocs de ce nœud légitime sur 2^{128} :

  $$P=\frac{Nbr_blocs}{2^{128}}$$

  Pour être plus précis, cette probabilité doit d'abord être multipliée par un autre paramètre, i.e. celui de la densité moyenne (nombre moyen de voisins) :

$$P=\frac{Nbr_blocs}{2^{128}} \times \text{densité moyenne}$$

Enfin, pour être exacte, un dernier paramètre doit être pris en compte. Il s'agit du taux d'acceptation qui permet de valider l'authentification du nœud. La probabilité sera donc égale à :

$$P=\frac{Nbr_blocs}{2^{128}} \times \text{densité moyenne} \times \text{taux d'acceptation}$$

Ceci indique que la probabilité qu'un nœud malveillant intègre le réseau est très faible, car les paramètres au numérateur sont très petits devant le dénominateur qui est trop grand. Donc nous pouvons en conclure que le protocole offre un très haut niveau de sécurité par rapport à ce type d'intrusion.

- Attaque par force brute

  Cette attaque est liée à l'intrusion des nœuds malveillants. Cette peut avoir lorsque le nœud malveillant parvient à avoir toutes les empreintes du réseau. De ce fait ils envoient beaucoup de requête pour atteindre le but principal c'est-à-dire qu'ils vont envoyer beaucoup de requêtes à ses voisins pour pouvoir être authentifier à la fin. La solution pour éviter cette attaque est qu'au bout de quelques tentatives infructueuses, les nœuds voisins vont blacklister ce nœud malicieux et ignorer simplement ses requêtes d'authentification. Cependant, le fait que les nœuds voisins effectuent cette action pourrait ne pas être très avantageux dans le cas où beaucoup de nœuds malicieux tenteraient d'être authentifiés en même temps, car les nœuds sont limités en termes de stockage.

- Attaque DoS/DDoS

  Cette attaque peut survenir lors de la phase d'initialisation et celle de l'authentification.

  Lors de la phase d'initialisation le serveur contenant les blocs secrets peut être atteint par ce type d'attaque l'empêchant de pouvoir mener à bien la collecte des informations d'un nœud ainsi que la distribution des différents blocs.

  Au niveau de la phase d'authentification, ce type d'attaque sera inexistant ou à défaut amoindrit par le fait que les requêtes des nœuds malicieux sont ignorées au bout de quelques tentatives infructueuses d'authentification (paramètre).

- Attaque Sybil
  Les objets de notre réseau ne possèdent qu'une seule identité et donc chaque nœud avec une identité possède sa propre paire de clé privée/publique. Lors de l'authentification d'un nœud, le message sera signé par les clés privées des nœuds, par conséquent, un attaquant ne peut pas utiliser de fausses identités pour mener cette attaque.
- Attaque par usurpation d'identité
  Un attaquant sera incapable de se faire passer pour un nœud du réseau car il doit avoir en sa possession la clé privée du nœud.
- Attaque Man in the middle
  Cette attaque ne peut pas survenir dans notre protocole car un attaquant ne sera pas capable de se mettre au milieu d'une communication entre deux nœuds et intercepté les messages venant d'un de ces nœuds. Il peut générer sa propre paire de clé privée/publique mais ne pourra pas détenir la clé privée du nœud pour déchiffrer le message qui lui est envoyé. En effet, ce message sera chiffré avec la clé publique du destinataire donc pour lire le message l'attaquant doit détenir la clé privée du destinataire ce qui n'est pas possible car cette clé est bien gardée.
- Attaque par rejeu
  Dans la phase d'authentification, un attaquant ne pourra utiliser un message car il doit posséder la clé du nœud pour la signer et l'envoyer. S'il génère sa propre clé cela ne correspondra pas à la clé privée du nœud pour calculer une fonction de hachage.

Comme nous pouvons le constater notre protocole est résistant à plusieurs d'attaques. Il garantit une robustesse qui est une exigence dans une conception de schéma d'authentification. Nous avons aussi fait son analyse par rapport à des critères qu'un concepteur de protocole d'authentification IoT doit au moins garantir.

❖ Analyse par rapport à certains critères de conception.

Tableau 7:Analyse du protocole par rapport à certains critères de sécurité

Spécificité du protocole	Utilisation de blocs de secrets qui authentifient des nœuds
Confidentialité	✓
Intégrité	✓
Authentification mutuelle	✓
Utilisation de clés cryptographiques	✓
Robustesse	✓
Scalabilité	✓
Confiance	✓
Décentralisation	✓
Autonomie	✓
Solution légère	✓
Mesure en termes de performance	Cette solution pourrait être un peu lourde si la densité du réseau est trop grande.

En clair, le protocole que nous avons proposé est meilleur que les protocoles précédents. Il remplit plusieurs critères qu'une méthode d'authentification doit garantir pour bien sécuriser les nœuds IoT.

6.8 Conclusion

Dans cette section nous avons proposé un nouveau protocole d'authentification pour les objets IoT. Ce protocole se base sur certains aspects de la blockchain comme la décentralisation, la confiance ou encore l'utilisation de systèmes cryptographiques pour permettre l'authentification des différents nœuds IoT dans un réseau. Nous avons par la suite fait son analyse selon plusieurs critères comme celle concernant les attaques. A la suite de ces analyses nous pouvons confirmer que notre protocole répondait à plusieurs critères de sécurité et est résistant à la plupart des attaques.

Conclusion Générale

L'Internet des objets représente une idéologie globale qui supprime les frontières entre le monde physique et le monde virtuel, et qui couvre la plupart des systèmes informatiques et technologies d'information. En effet, l'IoT regroupe plusieurs domaines tel que les réseaux de capteurs sans fil, les villes intelligentes, les véhicules connectés, les systèmes de contrôle commande, etc. De ce fait, un système IoT est un système hétérogène utilisant différentes technologies déployées sur des architectures et des plateformes différentes et implémentées sur des matériaux informatiques (hardware) très variés. Généralement, il utilise des technologies de communications sans fil afin de connecter des objets intelligents et autonomes. Ces objets ont la capacité de rassembler, analyser, traiter, générer et échanger des informations afin de fournir des services avancés. Cependant, les problèmes de sécurité informatique ralentissent considérablement l'évolution et le déploiement rapide de cette technologie de pointe.

L'authentification est un aspect important de la sécurité en général. Dans l'écosystème IoT, il est primordial, du fait que les nœuds de ce réseau augmentent de plus en plus. Ce qui implique que des nœuds malveillants peuvent accéder à des données privées. Il existe aujourd'hui plusieurs types d'attaques liées à l'authentification qui peuvent nuire comme l'attaque par usurpation d'identité.

Plusieurs méthodes d'authentification des nœuds ont été proposées pour répondre aux questions de sécurité. Cependant la plupart de ces solutions sont centralisées et souvent vulnérables face aux attaques de type DoS/DDoS. La technologie décentralisée offre d'énormes possibilités notamment sur les questions de la sécurité. De ce fait les chercheurs s'intéressent de plus en plus à cette technologie et ne cesse de proposer des protocoles et schémas d'authentification pour les objets connectés. Dans ce travail, nous avons passé en revue un bon nombre de ces protocoles et nous avons fait une analyse par rapport aux vulnérabilités des objets connectés. Ces méthodes ne peuvent cependant pas garantir une authentification à long terme à cause de l'évolutivité des objets connectés.

Pour pallier à ce problème, nous avons proposé un nouveau protocole d'authentification de sécurité robuste qui est conçu spécialement pour les systèmes IoT et adapté à leurs performances. Ce protocole se base sur les principaux atouts de la blockchain telles que la confiance et la décentralisation

du système. Il est résistant à plusieurs attaques liées à l'authentification et remplit plusieurs critères telles que l'intégrité, la confidentialité, etc.

REFERENCES

[1]. https://www.cairn.info/les-100-mots-de-l-internet--9782130592112-page-11.htm, consulté le 06/07/2021

[2]. file:///C:/Users/HP/Downloads/2016_Lascuritdesobjetsconnects_AuthorsVersion.pdf consulté le 09/07/2021.

[3]. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-F&type=items , consulté le 18/07/2021.

[4]. https://www.futura-sciences.com/tech/definitions/internet-internet-objets-15158/ , consulté le 22/07/2021.

[5]. https://technplay.com/histoire-definitions-objet-connecte/, consulté le 22/07/2021.

[6]. https://www.rtl.fr/actu/sciences-tech/nabaztag-le-grand-retour-du-lapin-connecte-7797734221 , consulté le 22/07/2021.

[7]. http://www.audentia-gestion.fr/cisco/internet-of-things-fr.pdf , consulté le 25/07/2021.

[8]. https://IoT-analytics.com/IoT-2020-in-review/, consulté le 03/08/2021.

[9]. https://www.al-enterprise.com/-/media/assets/internet/documents/IoT-for-healthcare-solutionbrief-fr.pdf, consulté le 12/08/2021.

[10]. https://www.digikey.fr/fr/resources/IoT-resource-center/agriculture, consulté le 17/08/2021.

[11]. https://www.opendatasoft.com/fr/blog/cest-quoi-la-smart-city-une-introduction-a-la-ville-intelligent , consulté le 20/08/2021.

[12]. https://www.al-enterprise.com/-/media/assets/internet/documents/IoT-for-transportation-solutionbrief-fr.pdf , consulté le 22/08/2021.

[13]. https://coreight.com/content/montres-bracelets-lunettes-vetements-connectes, consulté le 09/09/2021.

[14]. https://www.iaria.org/conferences2020/filesUBICOMM20/DmitryKorzun_Tutorial_SmartAssistance.pdf , consulté le 14/09/2021.

[15]. https://www.digitalcorner-wavestone.com/2016/04/salon-IoT-world-decryptage-de-lecosysteme-de-IIoT-2/, consulté le 16/09/2021.

[16]. © Springer Nature Switzerland AG 2019 49 K. S. Mohamed, The Era of Internet of Things, https://doi.org/10.1007/978-3-030-18133-8_3 , consulté le 22/09/2021.

[17]. https://www.slideshare.net/indravi/will-internet-of-things-IoT-be-secure-enough, consulté le 28/09/2021.

[18]. https://www.researchgate.net/publication/307945826 ,consulté le 28/09/2021.

[19]. Internet of Things: Architecture, Security and Applications July 2017 in International Advanced Engineering And Management; DOI:10.24999/IJOAEM/02070037 consulté le 15/10/2021

[20]. A Survey of Protocols and Standards for Internet of Things Tara Salman, Raj Jain Department of Computer Science and Engineering Washington University in St. Louis {Tara Salman, Jain} @wustl.edu, consulté le 19/10/2021

[21]. https://www.i-scoop.eu/internet-of-things-iot/iot-technology-stack-devices-gateways-platforms/, consulté le 23/10/2021

[22]. A Concise Review on Internet of Things (IoT)-Problems, Challenges and Opportunities :Laith Farhan, Rupak Kharel, Omprakash Kaiwartya, Marcela Quiroz-Castellanos and Ali Alissa ; 2018 11th in International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP) ; consulté le 06/11/2021 .

[23]. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pages 336–341. IEEE, 2015, consulté le 09/12/2021.

[24]. OWASP-IoT-Top-10-2018-final.pdf , consulté le 02/01/2022.

[25]. https://www.researchgate.net/publication/331557996 , consulté le 05/01/2021

[26]. P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K. R. Choo, “A lightweight machine learning-based authentication framework for smart IoT devices,” Information Sciences, vol. 484, pp. 255–268, consulté le 12/02/2022.

[27]. A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment consulté le 13/02/2021.

[28]. file:///C:/Users/HP/Downloads/CM1_39-52Szonieckyetcoll.pdf , consulté le 09/02/2022

[29]. BCoT Sentry: A Blockchain-Based Identity Authentication Framework for IoT Devices Liangqin Gong, Daniyal M. Alghazzawi and Li Cheng, consulté le 18/02/2022

[30]. La Blockchain pour les Nuls®, Édition limitée IBM Publié par John Wiley & Sons, Inc. 111 River St. Hoboken, NJ 07030-5774 www.wiley.com Copyright © 2018 John Wiley & Sons, Inc., consulté le 19/02/2022

[31]. A Taxonomy of Blockchain-Based Systems for Architecture Design Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), consulté le 20/02/2022.

[32]. https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/blockchain.html, consulté le 23/02/2022.

[33]. https://greenbull-campus.fr/immobilier/guide/patrimoine/diversifier/preuve-enjeu-ou-preuve-de-travail, consulté le 21/02/2022.

[34]. file:///C:/Users/HP/Downloads/CHAPITREIII-StateoftheartofBlockchain%20(1).pdf, consulté le 20/02/2022.

[35]. On blockchain and its integration with IoT. Challenges and opportunities Ana Reyna, Cristian Martin, Jaime Chen, Enrique Soler, Manuel Diaz Department of Languages and Computer Science, University of Malaga, Boulevard Louis Pasteur 35, 29071 Malaga, Spain, consulté le 22/02/2022.

[36]. Soumyashree S. Panda, Debasish Jena, Bhabendu Kumar Mohanta, Somula Ramasubbareddy, Mahmoud Daneshmand, Amir H. Gandomi: Authentication and Key Management in Distributed IoT Using Blockchain T echnology. IEEE Internet Things J. 8(16): 12947-12954 (2021), consulté le 23/02/2021.

[37]. https://www.researchgate.net/publication/326094774_Bubbles_of_Trust_a_decentralized_Blockchain-based_authentication_system_for_IoT,consulté le 23/02/2021.

[38]. https://www.researchgate.net/publication/337936071, consulté le 24/02/2021.

[39]. https://arxiv.org/abs/1706.01730, consulté le 25/02/2021.

[40]. https://www.researchgate.net/publication/341156419_Proposed_Authentication_Protocol_for_IoT_using_Blockchain_and_Fog_Nodes, consulté le 25/02/2021.