REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
IINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABOU-BEKR BELKAID – TLEMCEN

THÈSE LMD

Présentée à :

FACULTE DES SCIENCES – DEPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

DOCTORAT

Spécialité: *Informatique Distribuée et Réseaux (IDR)*

Par :

Mr Sebbah Abderrezzak

Sur le thème

Privacy dans l'IdO basée sur une approche cryptographique et non cryptographique

---

Soutenue publiquement le 07/04/2024 à Tlemcen devant le jury composé de :

Mr Merzoug Mohammed	MCA	Université de Tlemcen	Président
Mr Kadri Benamar	Professeur	Université de Tlemcen	Directeur de thèse
Mr Dennouni Nassim	MCA	Université de Tlemcen	Examinateur
Mr Haroun Errachid Adardour	MCA	Université de Chlef	Examinateur
Mr Moussaoui Djilali	MCA	Université de Tlemcen	Examinateur

Laboratoire de Système et Technologie de l'Information et de la Communication (STIC)
BP 119, 13000 Tlemcen - Algérie

REMERCIEMENT

Une thèse est le fruit d'un travail collectif et je profite de cette occasion pour exprimer ma profonde gratitude à toutes les personnes qui m'ont accompagnée et soutenue tout au long de cette aventure doctorale.

Je tiens tout particulièrement à remercier mon directeur de thèse, **Pr. Kadri Benamar**, pour son engagement sans faille et son encadrement précieux tout au long de ces années de recherche. Son soutien inestimable, ses conseils éclairés et sa disponibilité ont été des éléments clés de ma réussite.

Je tiens également à exprimer ma gratitude au **Mr. Merzoug Mohammed** de l'Université de Tlemcen pour avoir accepté d'être le rapporteur de ma thèse. Je remercie également le **Mr. Dennouni Nassim** de l'école superieur de mangment et **Mr. Haroun Errachid Adardour** de l'Université de Chlef et **Mr. Moussaoui Djilali** de l'université de Tlemcen d'avoir accepté d'évaluer mon travail en tant qu'examinateurs.

Mes remerciements s'adressent également à tous les membres du laboratoire de recherche des STIC. Leur contribution, leurs échanges fructueux et leur esprit de collaboration ont grandement enrichi mon expérience de recherche.

Je tiens à exprimer ma gratitude à mes parents, à mon épouse et à mes frères et sœurs pour leur soutien indéfectible, leur présence bienveillante et leur confiance inébranlable en mes capacités. Leurs encouragements constants ont été une source d'inspiration et de motivation tout au long de ce parcours exigeant.

Enfin, je voudrais remercier tous les membres de ma famille, mes amis et toutes les personnes qui, de près ou de loin, m'ont encouragé. Leur soutien moral, leurs encouragements et leurs précieux conseils ont été inestimables.

Je suis conscient que cette liste de remerciements ne peut être exhaustive, mais je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué de près ou de loin à la réalisation de cette thèse.

Résumé

L'Internet des Objets (IdO) a émergé comme un secteur dynamique de l'internet, capturant un intérêt significatif ces dernières années et ayant un impact transformationnel sur la société. Ce domaine, regroupant une gamme variée d'objets connectés de tailles diverses, offre une multitude d'applications dans des domaines allant de la domotique à l'agriculture, en passant par la sécurité, les transports et la santé. L'IdO vise à faciliter l'interaction entre les objets agissant comme des capteurs et des actionneurs, permettant ainsi le contrôle à distance des appareils intelligents via des connexions ouvertes. Néanmoins, cette ouverture expose les données sensibles à un large éventail de risques, les rendant vulnérables à diverses formes d'attaques. La sécurisation de ces réseaux représente un défi majeur, en particulier dans des environnements caractérisés par des ressources limitées et une diversité importante. Pour répondre à ces défis, nous proposons trois mécanismes de sécurité robustes pour les systèmes IdO, conçus pour contrer les menaces émanant des connexions ouvertes. L'évaluation de ces solutions, réalisée à l'aide de la logique de Burrows-Abadi-Needham (BAN) et de l'outil de validation automatisée AVISPA, démontre leur fiabilité, leur efficacité et leur adaptation aux spécificités des réseaux IdO, comparativement à d'autres techniques récentes similaires.

Mot clés: IdO, BAN Logic, Sécurité, Protection de la privée, AVISPA, Authentification.

Abstract

The Internet of Things (IdO) has emerged as a dynamic sector of the internet, garnering significant interest in recent years and exerting a transformative impact on society. This domain, encompassing a diverse range of connected devices of various sizes, offers a multitude of applications across domains ranging from home automation to agriculture, security, transportation, and healthcare. IdO aims to facilitate interaction among objects acting as sensors and actuators, enabling remote control of smart devices via open connections. However, this openness exposes sensitive data to a wide array of risks, rendering them vulnerable to various forms of attacks. Securing these networks poses a major challenge, especially in environments characterized by limited resources and significant diversity. To address these challenges, we propose three robust security mechanisms for IdO systems, designed to counter threats arising from open connections. Evaluation of these solutions, conducted using Burrows-Abadi-Needham (BAN) logic and the automated validation tool AVISPA, demonstrates their reliability, effectiveness, and adaptation to the specificities of IdO networks, compared to other similar recent techniques.

Key words: IdO, BAN Logic, Security, Privacy, AVISPA, Authentication.

ملخص

ظهر الإنترنت الأشياء كقطاع ديناميكي من الإنترنت، مجتذبا اهتمامًا كبيرًا في السنوات الأخيرة ومؤثرًا بشكل جذري على المجتمع. يشمل هذا المجال مجموعة متنوعة من الأجهزة المتصلة بأحجام مختلفة، ويوفر مجموعة متعددة من التطبيقات عبر مجالات تتراوح من التحكم المنزلي إلى الزراعة والأمن والنقل والرعاية الصحية. يهدف الإنترنت الأشياء إلى تسهيل التفاعل بين الأشياء التي تعمل كمستشعرات وأجهزة التحكم، مما يتيح التحكم عن بعد في الأجهزة الذكية عبر الاتصالات المفتوحة. ومع ذلك، تعرض هذه الانفتاحات البيانات الحساسة لمجموعة واسعة من المخاطر، مما يجعلها عرضة لأشكال مختلفة من الهجمات. توفير الأمان لهذه الشبكات يشكل تحديًا كبيرًا، خاصة في البيئات المميزة بالموارد المحدودة والتنوع الكبير. لمواجهة هذه التحديات، نقترح ثلاث آليات أمن قوية لأنظمة الإنترنت الأشياء ، مصممة لمواجهة التهديدات الناتجة عن الاتصالات المفتوحة. يُظهر تقييم هذه الحلول، الذي يتم باستخدام منطق Burrows-Abadi-Needham (BAN) وأداة التحقق الآلي AVISPA موثوقيتها وفاعليتها وتكييفها مع خصوصيات شبكات الإنترنت الأشياء ، مقارنة بتقنيات أخرى مماثلة متاحة حديثًا.

الكلمات المفتاحية :الإنترنت الأشياء ،منطق BAN ،الأمان ،الخصوصية ،AVISPA ،المصادقة.

Sommaire

Liste Des Figures

Liste Des Tableaux

Liste Des Acronymes

IdO	Internet Des Objets
MQTT	Message Queuing Telemetry Transport
COAP	Constrained Application Protocol
AMQP	Advanced Message Queuing Protocol
DDS	Data Distribution Service
RFID	Radio Frequency Identification
RSA	(Rivest-Shamir-Adleman) est un algorithme de cryptographie à clé publique
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
DSA	Digital Signature Algorithm
PKI	Public Key Infrastructure
AC	Autorité de Certification
AE	L'Autorité d'Enregistrement
AD	L'Autorité de Dépôt (ou Repository)
EF	L'Entité Finale (EE)
MD5	Message Digest Algorithm 5
SHA	Secure Hash Algorithm
GWN	Gateway/Passerelle
Ui	User/Utilisateur
Sj	Sensor/ Dispositif IdO
XoR	(eXclusive OR) est une opération logique
VPN	Virtual Private Network
RCL	Répertoire destiné aux Certificats à Long Terme
RRCT	Répertoire réservé aux Certificats Temporaires
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAN Logic	Burrows, Abadi, Needham Logic
HLPSL	High Level Protocol Specification Language
Bio	Les empreintes digitales

Liste Des Publications

—A Privacy and Authentication Scheme for IdO Environments Using ECC and Fuzzy Extractor
Auteur(s) : A. Sebbah et B. Kadri;
Conférence : IEEE 2020 International Conference on Intelligent Systems and Computer Vision (ISCV);
Lieu : Fez, Morocco;
Date : 2020;
Catégorie : Article de revue ;
Domaine(s) : Informatique ;
Langue : Anglais ;
Audience : internationale ;
État : publié.

— Security Issues in the Internet of Things
Auteur(s) : Sebbah, A., Kadri, B;
Revue : International Conference on Managing Business Through Web Analytics . Springer, Cham;
Date : 2022 ;
Catégorie : Chapter ;
Domaine(s) : Informatique ;
Langue : Anglais ;
Audience : internationale ;
État : publié.

— A Strong ECC Based on Secure Authentication with Privacy for IdO Concepts: Using Fuzzy Extractor
Auteur(s) : Sebbah Abderrezzak, Kadri Benamar;
Revue : International Journal of Technology Diffusion (IJTD);
Date : 2022/1/1 ;
Catégorie : Article de revue;
Langue : Anglais ;
État : publié.

— Cryptanalysis of an Authenticated Establishment Key System for Internet of Drones incorporates Privacy Using ECC and 5G Technology
Auteur(s) : Sebbah Abderrezzak, Kadri Benamar;
Revue : Journal of High Speed Networks;
Date : 2023 ;
Catégorie : Article de revue;
Langue : Anglais ;
État : soumis.

— Privacy dans l’IdO basée sur une approche cryptographique
Auteur(s) : Sebbah Abderrezzak, Kadri Benamar;

Conférence : JSTIC_2018, 2019, 2020, 2022 ;
Lieu : Tlemcen, Algérie ;
Catégorie : Poster ;
Langue : Anglais, Français;
Audience : nationale ;
État : publié.

Introduction Générale

L'internet des objets (IdO) représente une évolution majeure de l'internet traditionnel et des réseaux de capteurs et d'actionneurs sans fil. Il permet à tous les objets et équipements physiques d'être connectés à l'internet et d'interagir avec le réseau. Dans cette vision de l'IdO, des équipements tels que les téléphones portables, les réfrigérateurs, les montres, les appareils de climatisation, les appareils de mesure de l'électricité, du gaz et de l'eau, ainsi que les portes et les fenêtres, peuvent être connectés à l'internet, générant une quantité considérable de données qui pourraient être liées directement ou indirectement à leurs utilisateurs par exemple(emplacement, habitudes, présence/absence, heures d'éveil et de sommeil, régimes alimentaires, etc).

A partir de là, pour préserver la Privacy et la vie personnelle des personnes qui sont liées de différentes façons à ces équipements, le principe de la protection de la Privacy a été mis en place. Il se résume à des droits fondamentaux de l'utilisateur : Par l'authentification, est le processus de vérification de l'identité d'un objet connecté ou d'un utilisateur dans un environnement IdO. Cela garantit que seuls les objets ou les utilisateurs autorisés pourront accéder aux ressources et aux services offerts. L'authentification peut être réalisée à l'aide de techniques telles que les clés d'identification, les certificats numériques ou les protocoles d'échange sécurisés. La protection de la vie privée joue également un rôle important dans l'IdO. Elle a pour but de préserver la confidentialité des données personnelles et des informations des utilisateurs. Les données collectées par les objets connectés ne doivent donc pas être divisées, ni utilisées ou exploitées sans le accord et à l'insu de l'utilisateur.

Cette thèse se concentre sur le sujet de la confidentialité et de l'authentification dans les objets connectés (IdO). Dans un premier temps, nous analysons les solutions existantes et ensuite, nous proposons une nouvelle approche qui combine ECC et Fuzzy Extractor afin de renforcer la sécurité des nœuds face à diverses attaques, tout en préservant la confidentialité des données

Cette thèse est organisée en deux parties distinctes. La première partie aborde l'état de l'art et la théorie de l'Internet des objets (IdO), tandis que la seconde partie présente les contributions de l'auteur. La première partie se compose de deux chapitres qui offrent une description approfondie de l'IdO en général, de la sécurité dans l'IdO et de l'état de l'art. Cette partie fournit une introduction détaillée aux questions générales abordées dans la thèse.

Le premier chapitre présente une introduction à l'Internet des objets et explore les divers domaines d'application ainsi que les protocoles de communication utilisés dans l'Internet des objets tels que MQTT, COAP, AMQP, etc. De plus, une attention particulière est

accordée aux défis en matière de sécurité et de normalisation et l'hétérogénéité, etc. dans le domaine de l'Internet des objets.

Le deuxième chapitre se concentre spécifiquement sur les problématiques de sécurité propres à l'Internet des objets. Il examine ensuite différentes mécanismes de sécurité à faible consommation d'énergie, et moins coûteux en termes de calcul et de communication, basés notamment sur les fonctions et arbres de hachage, les chaînes de clés à sens unique, les formes cryptographiques, en mettant en évidence leurs avantages et leurs limitations dans le contexte de l'IdO.

Dans le Troisiéme chapitre, nous présentons une nouvelle approche visant à assurer la confidentialité, l'intégrité, l'authentification de l'utilisateur et la protection de leur vie privée. Pour cela, nous avons introduit deux types de clés basées sur les courbes elliptiques (ECDH) : les clés certifiées à long terme, associées à l'identité, et les Alias anonymes temporaires, générés de manière dynamique. Ces Alias sont enregistrés de manière transparente par l'autorité de certification, qui maintient deux répertoires distincts pour les clés à long terme et les clés temporaires.

Dans le quatrième chapitre, nous proposons un nouveau système d'authentification performant, offrant à la fois une sécurité optimale et une efficacité en termes de calcul et de communication. Ce protocole vise à garantir la sécurité des informations des capteurs IdO lors de leur diffusion et de leur stockage, en mettant en œuvre des méthodes de chiffrement et d'authentification robustes. À cet effet, nous utilisons le cryptage ECC pour la protection des données et le Fuzzy Extractor pour assurer l'authentification de l'utilisateur.

Enfin, le dernier chapitre est dédié à la multiplication scalaire sur les courbes elliptiques, opération fondamentale de tous les protocoles reposant sur ces objets mathématiques. Nous présentons une nouvelle méthode d'authentification et d'échange de clés pour l'internet des objets (IdO), utilisant l'algorithme de cryptographie à courbe elliptique (ECC) et un extracteur flou, tout en minimisant les coûts. Ce protocole vise à garantir la sécurité des données transmises et stockées par les capteurs de l'IdO en utilisant des techniques de cryptage et d'authentification robustes. Nous recourons à la cryptographie ECC et à l'extracteur flou pour protéger les données et assurer l'authentification mutuelle entre les différents nœuds.

CHAPITRE 1 : INTRODUCTION SUR L'INTERNET DES OBJETS

1.1 INTRODUCTION

L'internet des objets (IdO) est un réseau de terminaux (objets) hautement connectés. L'IdO relie le monde physique au monde virtuel, offre un large ensemble d'options et d'applications dans différents domaines, tels que la maison intelligente, l'agriculture, la sécurité, les transports et les questions de santé. Du point de vue actuel, l'IdO inclut divers types de dispositifs, par exemple des capteurs, des actionneurs, des étiquettes RFID ou des smart-phones, qui sont très différents en termes de taille, de poids, de fonctionnalités et de capacités. Gartner prévoit qu'il y aura plus de 50 milliards d'objets connectés sur le marché d'ici 2020 (voir la figure 1.1). Nous assistons à une véritable révolution numérique qui va radicalement changer notre façon de vivre [1-2] en raison des différents domaines d'application touchés par l'IdO.

Dans ce chapitre, nous présentons d'abord l'IdO, son architecture, ainsi que les vulnérabilités et les Problématiques posées par l'Internet des objets. Nous consacrons par la suite le reste du chapitre a la définition de quelques notions utilisées dans le domaine de la sécurité et enfin, nous allons finir par une conclusion.

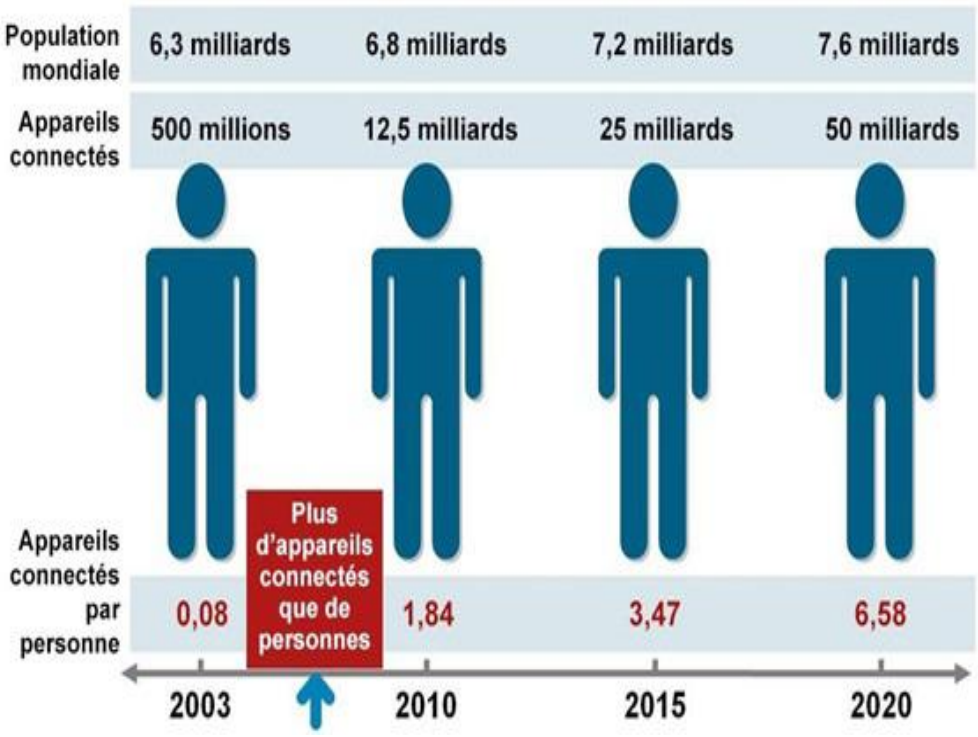

Fig 1.1. IdO entre 2003 et 2020 [3].

1.2 DEFINITION DE L'IdO

L'Internet des objets (IdO) est un concept qui a été introduit pour la première fois par Kevin Ashton et al en 2009 et qui est devenu de plus en plus prédominant dans notre société actuelle. Les dispositifs IdO sont des objets connectés dotés de capteurs, de logiciels et de connectivité réseau, qui permettent de collecter et d'échanger des données. Selon les estimations de Gartner [4], l'IdO a atteint plus de 60 milliards d'unités déployées en 2025, ce qui démontre son ampleur croissante dans notre monde moderne.

Le principal obstacle de l'internet des objets est de faire fonctionner ces gadgets sur l'internet conventionnel. C'est pourquoi les efforts de recherche récents se sont concentrés sur la création de nouveaux protocoles pour résoudre ce problème. L'internet des objets (IdO) est une infrastructure de pré-déploiement importante d'un réseau mondial qui se caractérise par des objets physiques reliés entre eux, dotés de leur propre identité numérique et capables de communiquer entre eux. Comme le montre la figure 1.2, le réseau établit un pont entre les mondes réel et virtuel, permettant l'automatisation et la gestion de divers systèmes et processus tels que les maisons intelligentes, les systèmes de contrôle industriels et les réseaux de transport.

D'un point de vue technique, l'IdO consiste en une identification numérique directe et standardisée d'objets physiques (adresses IP, protocoles SMTP, HTTP, etc.) grâce à des systèmes de communication sans fil tels que les puces RFID, Bluetooth et Wi-Fi [5]. Cette auto-configuration globale du réseau signifie que tous les différents types de capteurs, actionneurs et autres périphériques embarqués peuvent se connecter au réseau. Les applications de l'IdO sont multiples, allant de l'industrie à l'agriculture, en passant par la sécurité, les maisons intelligentes, les transports et la santé. Les dispositifs IdO sont déployés à l'extérieur pour contrôler et signaler les changements dans l'environnement.

En conclusion, l'internet des objets est un concept qui permettra un partage transparent des données et une communication entre les objets, transformant notre monde en un monde plus connecté et plus efficace. Mais il reste des obstacles à surmonter pour que l'IdO soit utilisé au mieux, comme la sécurité des données, la gestion des protocoles et l'interopérabilité des appareils. Ces difficultés seront abordées dans cette thèse.

Fig 1.2. Représentation de L'internet des Objets?

1.3 STRUCTURE D'UN OBJET CONNECTE

Les objets connectés peuvent collecter, stocker, traiter et transmettre des informations sur l'environnement qu'ils surveillent. Chacune de ces fonctionnalités est décrite ci-dessous.

1.3.1 Collection des données

Cette unité permet aux données d'être reconnues et récupérées par différents objets de l'environnement. Par exemple, en télémédecine, des capteurs attachés au corps du patient commencent à collecter des données sur des conditions de santé telles que la température, la pression artérielle, la glycémie, etc.

1.3.2 Stockage des données

Cette deuxième permet d'enregistrer les Données collectées lors de la phase précédente sous forme brute dans la mémoire de l'objet. S'il y a suffisamment d'espace, sinon il sera enregistré dans le Cloud.

1.3.3 Traitement d'informations

Ce processus peut intervenir à tout moment depuis la collecte des données jusqu'à leur retour à l'utilisateur final. Cette phase analyse et traite les données enregistrées lors de la phase précédente.

1.3.4 Transmission et la Délivrance des données

La transmission de données s'effectue à toutes les phases, notamment entre les objets et le Cloud, les objets et les utilisateurs finaux. La Délivrance consiste en la présentation d'informations d'une manière compréhensible pour les utilisateurs. En d'autres termes, La Délivrance rapide et sans erreur des données du traitement aux utilisateurs finaux.

1.4 STRUCTURE DE l'IdO

L'architecture d'un système IdO est cruciale pour garantir la performance et l'évolutivité du système. Il existe de nombreux modèles d'architecture IdO différents, mais un des modèles d'architecture les plus populaires est l'architecture en couches qui se composent de différentes couches qui permettent la connectivité, la gestion de données et l'application. La couche de connectivité permet la communication entre les objets connectés et les autres éléments de l'architecture, tels que les passerelles et les serveurs. La couche de gestion de données permet la collecte, le stockage et l'analyse des données collectées par les objets connectés. La couche d'application permet la création de services et d'applications qui utilisent les données collectées pour offrir des fonctionnalités supplémentaires.

Il est important de noter que les objets connectés, les passerelles, les serveurs et les utilisateurs sont les éléments fondamentaux d'un système IdO, ils travaillent ensemble pour permettre la collecte, le traitement et la distribution des données pour des utilisations variées.

1.4.1 Les objets connectés

Sont les éléments physiques de l'IdO, tels que les capteurs, les actionneurs et les périphériques embarqués. Ils sont équipés de capteurs et de moyens de communication pour collecter et transmettre des données. Les objets connectés peuvent varier considérablement en termes de taille, de forme et de fonctionnalité, mais ils ont tous en commun la capacité à se connecter à d'autres dispositifs et à échanger des données.

1.4.2 Les passerelles

Sont des dispositifs qui permettent la communication entre les objets connectés et les autres composants de l'architecture IdO. Les passerelles peuvent être utilisées pour connecter les objets connectés à des réseaux privés ou publics, ou pour convertir les protocoles de communication entre les objets connectés et les autres composants de l'architecture.

1.4.3 Les serveurs

Sont des dispositifs qui permettent la collecte, le traitement et la distribution des données des objets connectés. Ils peuvent également être utilisés pour stocker les données, pour effectuer des analyses et pour fournir des services d'application. Les serveurs peuvent être situés dans des centres de données ou dans le cloud, selon les besoins de l'application.

1.4.4 Les utilisateurs

Sont les personnes qui interagissent avec les objets connectés et les autres composants de l'architecture IdO. Les utilisateurs peuvent être des personnes physiques ou des systèmes automatisés qui utilisent les données collectées par les objets connectés pour prendre des décisions ou pour contrôler les objets connectés.

En somme, l'architecture d'un système IdO se compose de plusieurs couches qui permettent de connecter les objets connectés aux réseaux privés ou publics, et de communiquer entre eux. Les objets connectés, les passerelles, les serveurs et les utilisateurs sont les composants fondamentaux d'un système IdO, ils travaillent ensemble pour permettre la collecte, le traitement et la distribution des données pour des utilisations variées.

1.5 DIFFERENTES COUCHE DE L'IdO

Sur le plan architectural, les trois principaux niveaux d'organisation de l'Internet des objets sont la couche applicative, la couche réseau et la couche de perception donnée [6]. La figure 1.3 ci-dessous illustre cette organisation.

1.5.1 Couche de perception des données

Cette couche est constituée des capteurs et des outils de collecte de données qui mesurent les données de l'environnement physique, telles que les températures, les mouvements et les niveaux de lumière. Les dispositifs de cette couche transmettent les données au réseau IdO à l'aide de protocoles tels que ZigBee, Bluetooth Low Energy (BLE) et 6LoWPAN [7].

1.5.2 Couche réseau

Cette couche contrôle la façon dont les dispositifs IdO communiquent entre eux. Pour assurer un transfert de données fiable et sécurisé, elle utilise des protocoles de transport tels que TCP/IP, MQTT et CoAP. Les passerelles, les routeurs et les serveurs qui relient les dispositifs IdO à d'autres réseaux, y compris l'Internet, peuvent également être inclus dans la couche réseau [7].

1.5.3 Couche support

Les appareils d'un système IdO qui sont reliés et communiquent entre eux peuvent produire une variété de services au niveau de la couche support. L'administration des services et l'archivage des données pour les informations des couches inférieures sont les deux principales tâches de la couche support. Cette couche a également la capacité d'extraire, de traiter, de calculer, puis de prendre ses propres décisions en fonction des résultats de ces calculs.

1.5.4 Couche application

Cette couche est constituée de programmes qui utilisent les informations recueillies par les appareils IdO pour exécuter des fonctions particulières. Les programmes de gestion de la maintenance prédictive, par exemple, peuvent utiliser les données de mouvement pour détecter les anomalies et prévoir les pannes, tandis que les applications de domotique peuvent utiliser les données de température pour contrôler la température d'une maison. Les applications de la couche applicative peuvent fonctionner sur les ordinateurs, les téléphones mobiles, les ordinateurs de bureau et les serveurs en nuage [7].

Ensemble, ces trois couches permettent à l'internet des objets de fonctionner de manière efficace et fiable tout en recueillant et en utilisant des données à des fins diverses.

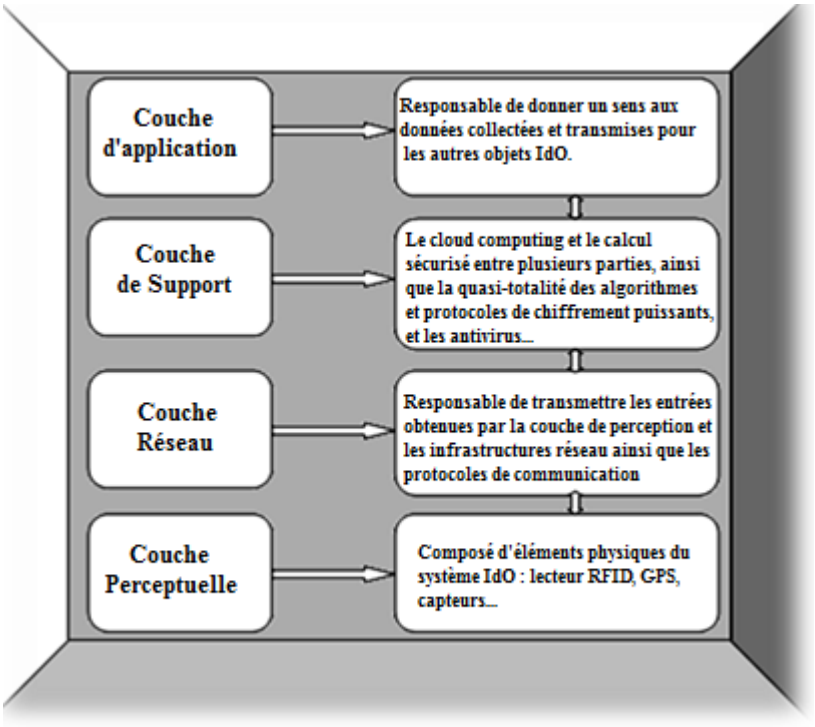

Fig 1.3. Les différentes couches de l'Internet des objets (IdO)

1.6 DOMAINES D'APPLICATION DE L'IdO

L'internet des objets offre un large choix d'options et d'applications dans différents domaines, tels que les maisons/villes intelligentes, l'agriculture, la sécurité, les transports et la santé, etc.

1.6.1 Les Maisons intelligentes

Regroupe un ensemble de dispositifs intelligents déployés à domicile et communiquant localement par des canaux sans fil. Il est possible d'accéder à distance aux dispositifs domestiques par l'intermédiaire d'une passerelle domestique. Par exemple, dans ce scénario, vous pouvez préparer votre café au lever, contrôler la température de la pièce,

ajuster la qualité de l'air et même programmer le chauffage de votre dîner avant votre retour à la maison, tout cela à l'aide de votre téléphone intelligent [8].

1.6.2 L'industrie intelligente

L'Internet des objets (IdO) a considérablement affecté l'industrie de la fabrication et a permis de développer ce que l'on appelle désormais l'industrie 4.0 ou l'industrie intelligente. L'Internet industriel des objets (IIdO) permet de surveiller en temps réel les processus de fabrication, d'optimiser la chaîne d'approvisionnement et d'améliorer la qualité du produit final en utilisant des capteurs connectés, des technologies de l'information et de la communication (TIC) et des algorithmes de traitement des données, L'IIdO a pour but à fournir un meilleur contrôle sur les processus de production, les données et les enjeux afin de fournir un produit final efficace et fiable [8].

Enfin et surtout, l'IIdO permet de réduire les coûts grâce à l'automatisation et à la surveillance en temps réel des processus, ce qui permet de détecter et de corriger rapidement les anomalies et de réduire par conséquent les pertes liées à la production.

1.6.3 Le système de santé intelligent

L'Internet des objets a révolutionné le monde de la santé et a permis de développer ce que l'on appelle désormais IMoT ou système de santé intelligent, le système se compose de plusieurs éléments (Patients, médecins, infermières, etc.) et différents objets (capteurs, montres, Smartphones, etc.) et les applications ou interfaces. Ce système collecte, transmet et stocke les informations physiologiques des patients.

Par exemple, un capteur médical peut enregistrer la fréquence cardiaque d'un patient et l'envoyer à un serveur hospitalier pour diagnostic et surveillance [8].

1.6.4 Agriculture intelligente

Un domaine en développement des technologies de l'information appelé "agriculture intelligente" cherche à améliorer les méthodes agricoles et à augmenter les rendements tout en minimisant les déchets. L'agriculture intelligente s'appuie sur les dernières technologies pour augmenter considérablement la productivité. L'agriculture intelligente utilise des capteurs, des algorithmes de traitement des données et des technologies de communication pour permettre la surveillance en temps réel des conditions microclimatiques, de l'humidité du sol, de l'irrigation et de la température, ce qui peut contribuer à garantir la qualité des aliments. En outre, l'agriculture intelligente peut intégrer la surveillance des terres pour détecter les maladies et les parasites susceptibles d'avoir un impact sur les cultures, ainsi que la surveillance de la faune pour prévenir les conflits entre les activités agricoles et les animaux. La collecte, l'analyse et l'application des données à l'aide des technologies de l'information peuvent également conduire à une augmentation de la production, à une baisse des prix et à une amélioration des produits alimentaires, ainsi que Les capteurs pourraient être reliés aux animaux sauvages dans un système agricole intelligent pour suivre leur comportement et leur santé [9]. Enfin, l'agriculture intelligente peut jouer un rôle crucial dans la réalisation de l'objectif

consistant à assurer une alimentation saine et abondante à une population mondiale en constante augmentation. Il est essentiel de souligner que la mise en œuvre de l'agriculture intelligente posera des problèmes en termes de coûts, de confidentialité des données et de durabilité environnementale. Par conséquent, pour atteindre les objectifs du développement durable, des recherches doivent être menées pour améliorer ces technologies et veiller à ce qu'elles soient utilisées de manière responsable.

1.6.5 **Les services publics**

Sont ceux qui sont offerts par les gouvernements au profit du grand public. Ces infrastructures publiques, comme les réseaux d'eau et d'électricité, peuvent être surveillées à l'aide de capteurs et de gadgets IdO (Internet des objets). Ces capteurs et dispositifs IdO peuvent être utilisés pour surveiller et détecter les fuites ou les risques de coupures de courant.

La détection des surtensions ou des interruptions de courant prospectives est rendue possible par cette surveillance, ce qui peut contribuer à limiter les dommages et les perturbations pour les consommateurs de services. Grâce à ces technologies, les gouvernements peuvent améliorer la norme et la fiabilité des services qu'ils fournissent au public.

1.6.6 **La sécurité**

En permettant la surveillance en temps réel de divers lieux publics, les capteurs IdO peuvent en fait, contribuer à accroître la sécurité publique. Les autorités peuvent prendre des mesures pour mettre fin aux crimes et aux incidents en utilisant les données générées par les capteurs pour repérer les activités suspectes et les anomalies. Il est crucial de se rappeler que la sécurité des dispositifs IdO est une préoccupation sérieuse, et que pour prévenir les cyber attaques et les violations de la vie privée, des mesures de sécurité appropriées doivent être mises en œuvre [8].

1.7 LES DÉFIS DE L'IdO

En ce qui concerne leur taille, les applications et l'environnement de déploiement, l'IdO est confronté à plusieurs problèmes tels que l'hétérogénéité, l'impact du monde physique, la sécurité et la confidentialité des individus, la définition des normes, la capacité de la batterie et la puissance de calcul, la complexité [10].

1.7.1 **Autonomie prolongée de la batterie**

En général, les dispositifs IdO sont alimentés sont caractérisés par une puissance de batterie limitée, ce qui rend l'utilisation d'un protocole de sécurité avancé et complexe très coûteuse. Par conséquent, tout mécanisme de sécurité développé doit prendre en considération l'aspect de la batterie.

Dans certaines situations, un autre problème apparaît : il est impossible de recharger la batterie, il convient donc de trouver un moyen de générer de l'énergie à partir de l'environnement (lumière, chaleur, vibrations, etc…).

1.7.2 Les normes

L'internet des objets est au centre de toutes les technologies et développements modernes. Bien que le défi majeur soit de gérer l'hétérogénéité des objets et des normes couplée à une multitude d'applications.

1.7.3 Hétérogénéité

L'Internet des objets est composé de la diversité des composants matériels et logiciels utilisés pour construire des objets. Ils n'utilisent pas les mêmes systèmes d'exploitation et n'ont pas les mêmes interfaces de communication. Ce qui entraîne une importante l'hétérogénéité technique.

1.7.4 Sécurité/confidentialité

Les technologies contemporaines de sécurité, telles que le cryptage, l'authentification, l'échange de clés, la signature, etc., sont mal adaptées à l'environnement IdO, exposant ainsi les objets à diverses attaques et mettant en péril la sécurité des biens et des personnes. Bien que ces technologies aient proposé différentes normes et protocoles pour assurer la sécurité et la confidentialité des utilisateurs, leur efficacité demeure limitée en raison de la diversité des attaques ciblant les capteurs.

1.8 PROTOCOLES IdO

Dans cette section, nous présentons les protocoles IdO divisés en deux catégories : IdO-to cloud et IdO-to-fog.

1.8.1 IdO-TO-CLOUD

L'IdO interconnecté au nuage comprend les protocoles AMQP et DDS :

1.8.1.1 Protocole avancé de mise en file d'attente des messages (AMQP)

AMQP (Advanced Message Queuing Protocol) est un protocole de communication asynchrone à code source ouvert qui permet aux applications de communiquer via une file d'attente de messages. Ce protocole est basé sur l'utilisation du modèle de message de publication/abonnement. Un modèle de message de publication/abonnement qui achemine, enregistre et échange des messages au sein d'un courtier avec un ensemble de politiques pour les composants de câblage. Il définit une structure standard pour les échanges de messages entre applications, permettant l'interopérabilité entre différentes implémentations du protocole.

AMQP comprend les concepts suivants :

Producteur : une application qui publie des messages dans une file d'attente.
Consommateur : une application qui reçoit des messages d'une file d'attente.
File d'attente : une collection de messages publiés par un producteur et reçus par des consommateurs.
Canal : un tunnel logique pour les échanges de messages entre le producteur et les consommateurs.

AMQP offre des fonctionnalités telles que la gestion des transactions, la livraison garantie, la sélection des messages en fonction de critères et la gestion des files d'attente. Il est souvent utilisé pour mettre en œuvre des architectures distribuées pour les systèmes de messagerie, la gestion des événements et la communication entre micro services, garantissant ainsi l'intégrité des données. AMQP prend également en charge la sélection des messages en fonction de critères, ce qui signifie que les consommateurs peuvent choisir de ne recevoir que les messages qui répondent à certaines conditions, il utilise TCP pour un transport fiable et fournit un mécanisme de sécurité utilisant TLS pour le chiffrement et l'authentification [11], [12].

1.8.1.2 Service de distribution de données (DDS)

Le DDS est un protocole décentralisé basée à la connectivité entre pairs et au partage fiable et en temps réel des données. Ce modèle d'interaction est de type publish-subscribe. Lorsqu'il s'agit de fournir aux applications un service de haute qualité, ce protocole ne dépend pas du composant broker ou du multicast. L'utilisation d'algorithmes de contrôle de la qualité de service par DDS permet de gérer efficacement la livraison de données en temps réel via les réseaux, garantissant une transmission fiable des données même en présence de réseaux erratiques ou de limites de bande passante.

DDS offre aux applications la possibilité de s'abonner aux données pertinentes et de filtrer les données non pertinentes en plus de la livraison des données. Il offre également des fonctions de découverte des données, de filtrage des données et de publication et d'abonnement. Bien que le protocole TCP puisse être utilisé pour la sécurité, DDS utilise généralement le protocole UDP. TLS sur TCP et DTLS est utilisé sur UDP [11].

1.8.2 IdO- TO-FOG

L'IdO interconnecté au brouillard comprend les protocoles MQTT et CoAP :

1.8.2.1 Protocole de transport de télémétrie des files d'attente de messages (MQTT)

L'architecture de publication/abonnement, par opposition au paradigme demande/réponse HTTP, est le fondement du protocole de communication MQTT pour les systèmes d'objets connectés (IdO). MQTT est le protocole parfait pour les applications de l'Internet des objets (IdO) qui ont besoin de stabilité et de communication en temps réel, car il inclut également des capacités telles que la qualité de service, la gestion de la fiabilité des messages et la résolution des déconnexions temporaires. MQTT transmet des données en temps réel en

utilisant une architecture de publication/abonnement. Les clients publient des messages sur certains sujets, et d'autres clients peuvent s'abonner à ces sujets pour recevoir les messages publiés.

Dans MQTT, la communication entre l'émetteur et le récepteur s'effectue sur le réseau via le courtier. Comme les clients ne reçoivent que les données qui les intéressent, les éléments liés peuvent communiquer efficacement entre eux (voir la figure 1.4).

En résumé, MQTT utilise le protocole TCP pour la transmission sécurisée et un transport fiable [13].

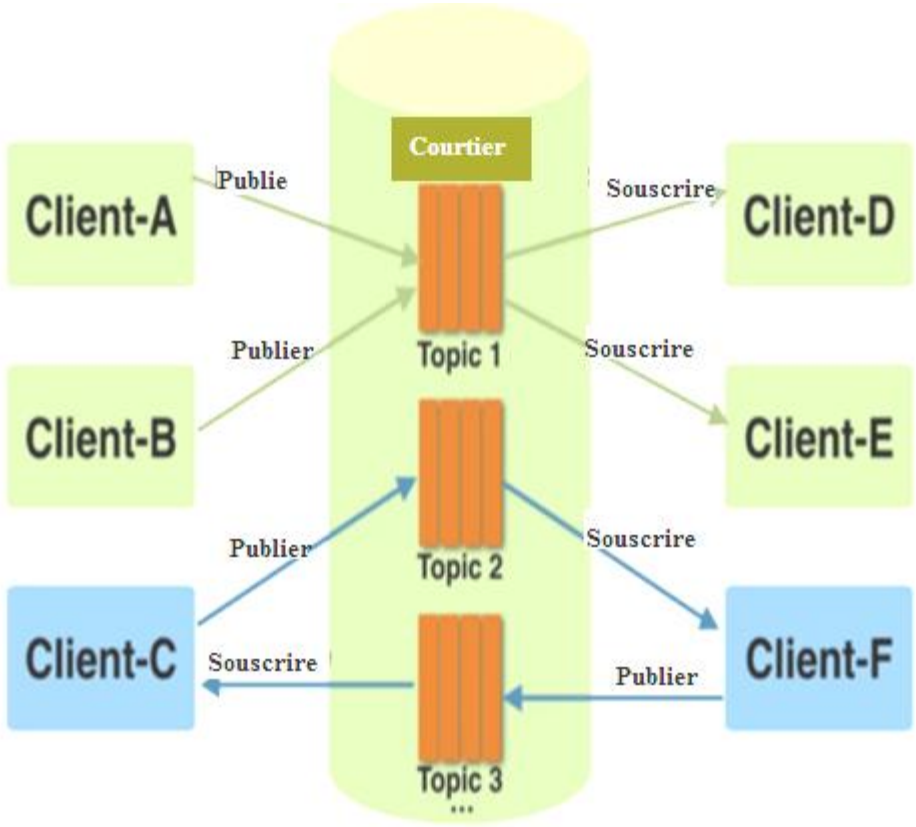

Fig 1.4. Fonctionnement de MQTT [14].

1.8.2.2 **Protocole d'application contraint (CoAP)**

CoAP est un protocole léger qui prend en charge le paradigme demande/réponse conçu pour le système IdO basé sur les protocoles HTTP qui utilise UDP pour un transport fiable. En outre, fournit un mécanisme de sécurité basé sur DTLS, l'échange de messages entre le client et le serveur se produit uniquement par des clés de cryptage.

Ce système est divisé en deux couches logiquement différentes, la première couche : appelée la couche de demande/réponse qui met en œuvre le paradigme RESTful. Et la deuxième couche est appelée couche structurelle destinée à retransmettre les paquets perdus [11].

1.9 LES TECHNOLOGIES CLES DE L'IdO

Deux technologies clés de l'IdO sont la RFID (Radio Frequency Identification) et les réseaux de capteurs.

1.9.1 La technologie RFID

Permet aux appareils de communiquer entre eux en utilisant des ondes radio pour échanger des informations. Elle s'intègre dans les systèmes de l'Internet des objets pour améliorer la collecte et le partage de données. Nous verrons dans ce chapitre comment ces deux technologies peuvent fonctionner de concert pour créer des systèmes plus performants [15].

Un objet identifiable est doté d'une étiquette ou d'un transpondeur, qui est un dispositif électronique appelé lecteur, et les informations sont transmises entre eux par radiofréquences cette technique de communication sans fil appelé (RFID). Les objets tels que les cartes d'identité, les marchandises, les animaux, etc., peuvent tous être dotés d'une étiquette RFID. La capacité d'une étiquette à soumettre une demande d'information lorsqu'un lecteur RFID est suffisamment proche d'elle. L'étiquette peut alors envoyer des données, notamment son numéro d'identification personnel, son adresse ou des informations précédemment enregistrées. La technologie RFID offre des avantages tels que le suivi des objets en temps réel, une automatisation accrue des procédures d'inventaire, une lecture plus rapide et plus précise que la lecture manuelle des codes à barres et une réduction des erreurs humaines. Les secteurs de la logistique, des soins de santé, de la sécurité, du transport, de la fabrication et bien d'autres encore utilisent largement la technologie RFID [15]. Le suivi des produits, la gestion des actifs, le traçage des aliments, la gestion des stocks et la gestion de la sécurité sont autant d'applications de la technologie RFID.

1.9.2 Les réseaux de capteurs

Sont des réseaux distribués de capteurs qui permettent la collecte de données à distance [16]. Les capteurs peuvent mesurer différentes variables telles que la température, l'humidité, la pression, la luminosité, entre autres [16]. Les réseaux de capteurs sont souvent utilisés dans des applications telles que la surveillance de l'environnement, la surveillance de la santé, la maintenance prédictive, entre autres [17].

1.10 CONCLUSION

En conclusion, ce chapitre a fourni une vision globale de l'internet des objets (IdO), abordant divers points essentiels de ce domaine en plein essor. Nous avons examiné les architectures proposées dans la littérature, les progrès de la recherche et du développement, les principaux systèmes et technologies utilisés sur le terrain, ainsi que les applications concrètes de l'IdO.

Nous avons constaté que l'IdO a un énorme potentiel pour transformer de nombreux secteurs, tels que l'industrie, l'agriculture, la santé, les villes intelligentes et les transports. Grâce à la collecte de données en temps réel, à l'automatisation des processus et à l'amélioration de l'efficacité opérationnelle, l'IdO ouvre de nouvelles perspectives et promet d'améliorer notre qualité de vie. Toutefois, nous avons également identifié plusieurs défis importants auxquels sont confrontés les systèmes IdO. La limitation des ressources, la gestion des protocoles, l'évolutivité, la gestion des données massives et, surtout, la sécurité sont autant de préoccupations majeures. En résumé, ce chapitre a permis de jeter les bases d'une meilleure appréhension de l'IdO, en mettant en évidence les possibilités et les défis qu'il présente.

CHAPITRE 2 : SECURITE DANS L'INTERNET DES OBJETS

2.1 INTRODUCTION

L'internet des objets (IdO) est considéré comme la direction que prendra l'internet à l'avenir. En connectant des milliards d'objets ensemble, il a ajouté un niveau supplémentaire de commodité et de confort. L'IdO désigne un réseau d'objets et d'appareils physiques qui sont connecté à des systèmes d'électronique, aux dispositifs (capteurs) et à la connectivité. Cela leur permet de collecter et de partager des informations. L'IdO a le potentiel de révolutionner de nombreuses facettes de notre vie, notamment les transports, la santé et la sécurité, car de plus en plus d'appareils sont connectés.

Cependant, alors que ces appareils capturent et transmettent des informations sensibles, la connectivité croissante présente aussi de nouveaux problèmes en matière de sécurité. Il est donc essentiel de préserver la sécurité des dispositifs IdO et des données qu'ils manipulent afin d'éviter les violations de données, les cyber attaques et les accès non autorisés, qui pourraient avoir des effets désastreux sur les individus et les organisations. La sécurité des systèmes IdO doit être prise en compte dès leur conception et leur mise en œuvre, et les failles de sécurité doivent être corrigées à l'aide de techniques telles que le cryptage, l'authentification sécurisée et les mises à jour logicielles et matérielles de routine.

L'internet des objets peut avoir une influence le monde entier et améliorer notre vie quotidienne si les bonnes mesures de sécurité sont mises en place.

2.2 SECURITE DANS L'IdO

Dans cette partie, nous aborderons les objectifs, les exigences et les mesures de sécurité comme « confidentialité, l'intégrité, l'authentification, la fraîcheur et la disponibilité ». La première ligne de protection est l'emploi de techniques conventionnelles comme l'authentification, le contrôle d'accès, le cryptage et la signature numérique. La confidentialité et l'intégrité des informations sont garanties par des méthodes de cryptage. Pour empêcher tout accès non autorisé, des mécanismes d'authentification et d'autorisation ont été mis en place. La préservation de l'anonymat et de la confidentialité des utilisateurs, ainsi que la qualité et la disponibilité des données, sont autant d'objectifs de la sécurité. Pour assurer ces objectifs de la sécurité informatique ya des procédures et des techniques appropriées doivent être utilisées.

2.2.1 Objectifs de la sécurité

Dans cette partie, nous présenterons les objectifs et les exigences de la sécurité:

- **Confidentialité :** La confidentialité d'un message est la garantie que seuls l'expéditeur et le destinataire peuvent le lire. L'utilisation de méthodes de cryptage garantit souvent cet élément. Ce composant fondamental de la sécurité informatique permet de s'assurer que les informations privées sont protégées en les rendant inaccessibles aux parties non autorisées. Cela peut être assuré par l'utilisation des exigences de cryptage telles que le chiffrement symétrique et

asymétrique des données pour protéger les données pendant leur utilisation et leur stockage [18].

- **L'intégrité :** Est définie comme la propriété qui donne au récepteur et à l'expéditeur la possibilité de détecter toute altération du message échangé, ou le moyen de garantir que les données ne sont pas modifiées que par la personne autorisée. L'intégrité désigne la protection des données contre toute modification, altération ou suppression non autorisée [19], est une composante essentielle de la sécurité informatique. Dans ce cas, l'intégrité des informations garantit que les données stockées ou transmises sont exactes et fiables, ce qui est essentiel pour la confidentialité et la confiance des utilisateurs. Les risques pour l'intégrité des données sont nombreux et peuvent inclure l'erreur humaine, les défaillances du système, les attaques de pirates et les virus informatiques. Diverses mesures de sécurité informatique peuvent être mises en place pour maintenir l'intégrité des données. Par exemple, l'utilisation du cryptage pour rendre les données inintelligibles aux parties non autorisées protège les données. Une autre option consiste à utiliser des contrôles d'intégrité des informations, qui confirment que les informations n'ont pas été modifiées depuis leur création. Les certificats numériques sont également utilisés pour garantir l'authenticité et l'intégrité des communications électroniques.
  En conclusion, l'intégrité est un élément clé de la sécurité informatique, qui garantit que les données restent exactes et fiables dans un monde de plus en plus numérique.

- **Authentification :** Cet objectif permet de contrôler et de vérifier l'identité prétendue d'une entité, ou l'origine d'un message, ou d'une donnée. Cet aspect est généralement assuré en utilisant la biométrie ou le cryptage asymétrique...etc. L'authenticité d'une entité est vérifiée par le processus d'authentification, qui consiste à confirmer que l'entité est bien qui ou ce qu'elle prétend être. Dans le monde physique, l'identification est une tâche de routine effectuée à l'aide de diverses techniques, telles que la reconnaissance faciale ou auditive. Les connexions entre objets étant fréquemment automatisées et sans participation humaine, l'authentification est encore plus cruciale dans le contexte de l'IdO. Une illustration remarquable de l'utilisation de l'authentification dans IdO est l'utilisation d'une carte de crédit utilisant la technologie NFC. Sans une authentification appropriée, un attaquant potentiel pourrait facilement utiliser le compte du client pour effectuer des achats frauduleux [20] [21].
  Il existe plusieurs méthodes d'authentification, notamment les mots de passe, les signatures numériques, les identifiants biométriques et les clés de session. Les trois méthodes standard d'identification sont " Qui êtes-vous ? ", " Qu'avez-vous ? " et " Qui connaissez-vous ? ". En raison des contraintes de ressources des objets, la deuxième méthode est fréquemment utilisée dans le contexte de l'IdO.

- **Fraîcheur :** La sécurité des communications électroniques dépend fortement de leur fraîcheur. Il s'agit de la capacité d'un attaquant à saboter une session déjà en cours en exploitant des communications périmées. Imaginez un attaquant qui parvient à intercepter des messages que les deux parties ont déjà échangés. Il pourrait alors utiliser ces messages pour tromper l'une des parties et interrompre la connexion en cours. Cet aspect traite de la possibilité pour les attaquants d'utiliser d'anciens messages pour rompre la session avec l'entité communicante. Il est crucial de s'assurer que les messages transmis sont à jour et distincts afin de contrer de telles attaques. C'est pourquoi des mesures de contrôle de la fraîcheur sont utilisées pour garantir l'exactitude et la légitimité des messages envoyés dans les deux sens, comme les horodatages ou les numéros de séquence.

- **Autorisation :** La méthode utilisée pour déterminer si un utilisateur est autorisé ou non à accéder à une certaine ressource ou à un certain élément d'information. Les entreprises peuvent réduire la probabilité d'une violation de la sécurité en s'assurant que seuls les utilisateurs disposant des autorisations appropriées peuvent accéder aux informations sensibles, en mettant en place des politiques d'autorisation rigoureuses. En ce qui le concerne, Le système de contrôle d'accès permet de s'assurer que les utilisateurs ne peuvent accéder qu'aux ressources et informations auxquelles ils ont été autorisés à accéder, et il limite leur accès aux informations qui ne sont pas nécessaires à leur travail.
  Les entreprises peuvent réduire les risques d'accès non autorisé, de violation de la confidentialité, de perte d'informations et d'interruption de service en garantissant des autorisations et des contrôles d'accès appropriés. Des mesures de sécurité comprenant la gestion des privilèges, l'authentification à deux facteurs, la gestion des identités et des accès (IAM), et le cryptage post-transactionnel contribuent à renforcer la sécurité des communications en garantissant une autorisation et un contrôle d'accès appropriés.

- **Disponibilité :** Il s'agit de la capacité d'un utilisateur à accéder à des données dans n'importe quelle situation, dans le bon format et dans un délai spécifié. La disponibilité est un élément crucial de la sécurité des communications électroniques. La capacité d'un système à être disponible et utilisable à tout moment par les utilisateurs autorisés est appelée disponibilité. Des systèmes efficaces de surveillance, de sauvegarde et de récupération doivent être mis en place par les prestataires de services de communication pour garantir le plus haut niveau de disponibilité. Ils doivent également mettre en action de solides politiques de sécurité pour se protéger des attaques par déni de service (DDoS) et d'autres types d'attaques susceptibles de nuire à la disponibilité des services de communication. En conclusion, la disponibilité est un élément clé de la sécurité,

et il est essentiel de mettre en pratique des mesures de sécurité efficaces pour garantir le plus haut niveau de disponibilité des services de communication.

- **Privacy :** D'une part, la confidentialité et l'intégrité des informations stockées doivent être assurées par différentes techniques de cryptage. D'autre part, la confidentialité de l'utilisateur, entendue comme la capacité de pouvoir assurer et garantir l'anonymat des utilisateurs et la préservation des données personnelles. Au-delà des données la sécurité et la qualité est une condition pour une adoption généralisée [18]. Ensuite, les mécanismes d'authentification et d'autorisation doivent être prévus pour empêcher les dispositifs ou les utilisateurs non autorisés d'accéder au système.

2.2.2 Techniques de sécurisation

Dans cette rubrique, nous présenterons les différentes techniques de sécurité :

2.2.2.1 **Cryptographie :** La Cryptographie signifié l'écriture caché, utilisé pour assurer la confidentialité en rendant les données illisibles pour des personnes non autorisées. Afin de convertir les communications de manière difficile à comprendre, la cryptographie fait référence à des procédures d'information et de communication sécurisées construites à partir de principes mathématiques et d'un ensemble de calculs basés sur des règles, appelés algorithmes. Ces algorithmes déterministes sont employés dans la création de clés cryptographiques, de signatures numériques, de préservations de la confidentialité des informations personnelles, de navigation sur Internet et de transactions sécurisées par courrier électronique et par carte de crédit.

La cryptographie a deux principales méthodes de cryptage : chiffrement symétrique (avec la clé secrète) et le chiffrement asymétrique (avec la clé publique) [22].

- *Cryptage Symétrique :* Le cryptage symétrique est un type de cryptage fréquemment utilisé dans les ordinateurs pour préserver le secret des données. Cette approche repose sur l'utilisation d'une seule clé de chiffrement qui peut être utilisée à la fois pour le chiffrement et le déchiffrement des données.

  Le cryptage symétrique présente les avantages de la rapidité et de la simplicité, notamment pour les applications nécessitant un traitement rapide des données. Les algorithmes de cryptage symétrique sont préférables aux méthodes de cryptage asymétrique car ils sont souvent plus rapides. Le cryptage symétrique est très simple à mettre en place et à utiliser puisqu'une seule clé est nécessaire pour crypter et décoder les données. Cependant, Le plus gros inconvénient est l'obligation pour l'expéditeur et le destinataire d'échanger la clé de cryptage, ce qui peut entraîner des problèmes de sécurité si la clé est saisie par une personne

non autorisée. Le chiffrement symétrique ne garantit pas non plus l'intégrité des données qu'il chiffre, car toute personne possédant la clé de chiffrement à la possibilité de modifier les données avant de les déchiffrer.

En bref, la cryptographie symétrique est une méthode de cryptage simple et rapide qui peut être appliquée à une variété d'applications nécessitant la sécurité des données. Mais il est important de connaître ses limites et ses risques, notamment en ce qui concerne la protection de la confidentialité des données cryptées et la divulgation de la clé de cryptage.

Il existe un grand nombre d'algorithmes de cryptographie symétrique [23] :

- Chiffre de Vernam
- DES
- 3DES
- Chiffrement par blocs AES
- RC4
- RC5
- MISTY1

- *Chiffrement Asymétrique :* Lorsqu'il y a beaucoup de nœuds, comme dans les réseaux de capteurs, IdO, les techniques cryptographiques asymétriques peuvent offrir des solutions de sécurité efficaces. Le cryptage asymétrique utilise deux clés différentes (la clé privée/ la clé publique) pour crypter et décrypter les données. La clé publique est largement disponible et peut être utilisée par n'importe qui pour calculer des données destinées à son propriétaire. En revanche, le propriétaire de la clé privée la garde secrète et l'utilise pour décrypter des données qui ont été compromises à l'aide de la clé publique. Cryptographie asymétrique utilisé pour l'authentification et la signature électronique en associant une clé publique à une clé privée pour signer et vérifier les messages. Par rapport au chiffrement symétrique, le chiffrement asymétrique présente un certain nombre d'avantages. Dans un premier temps, la communication sécurisée entre des personnes inconnues est rendue possible par la capacité de la clé publique à être largement diffusée. Le cryptage asymétrique garantit également la validité et le secret des données envoyées.

  En effet, n'importe qui a la possibilité d'utiliser sa clé privée pour signer numériquement un message, établissant ainsi sa légitimité, alors que n'importe qui d'autre a la possibilité d'utiliser sa clé publique pour vérifier une signature [23].

  Pour une petite comparaison entre ECC et RSA : une clé ECC de 256 bits offre le même niveau de protection qu'une clé RSA de 3072 bits. L'utilisation de clés plus petites signifie qu'elle consomme moins d'espace de stockage et de bande passante pendant la transmission [24]. Les inconvénients du chiffrement asymétrique sont les suivants : Sont souvent plus lents que les algorithmes de chiffrement symétrique, ce qui peut poser des problèmes pour les applications nécessitant un traitement rapide des données. De plus, comme il nécessite la

gestion de deux clés distinctes, le chiffrement asymétrique est plus difficile à mettre en œuvre que le chiffrement symétrique. Enfin, le cryptage asymétrique peut être vulnérable à certaines attaques, telles que les attaques de type "man in the middle", qui peuvent permettre à un attaquant de modifier les données sans être remarqué. Il existe des algorithmes de cryptages asymétrique tel que :

- RSA (nommé par les initiales de ses trois inventeurs)
- ECC (elliptic curve cryptography).
- DSA
- Protocole d'échange de clés Diffie-Hellman

2.2.2.2 **Hachage :** Une fonction appelée "hachage" est une fonction qui permet de découper un grand ensemble en une collection plus petite d'empreintes digitales. Utilisé pour garantir l'intégrité en créant une empreinte numérique d'un message ou de données, qui peuvent être comparée pour vérifier que les informations (données) n'ont pas été altérées. Cette fonction n'est pas une méthode de cryptage, car elle ne peut pas faire l'objet d'un cryptage inverse pour récupérer l'ensemble original [25].

Quelques exemples d'algorithmes de hachage populaires sont MD5, SHA-1.

En définit une fonction de hachage :

Soit Σ un alphabet. Une fonction de hachage est désignée sous le nom d'application [25].

$$h : \Sigma^* \rightarrow \Sigma^n, n \in N$$

Par conséquent, les fonctions de hachage s'associent à des chaînes de caractères de longueur quelconque et à d'autres chaînes de caractères de longueur fixe. Nous tenons à vous signaler qu'elles ne sont pas encore injectables.

Un Exemple. L'application associant :

(1) $b1 \oplus b2 \oplus \ldots \oplus b_n$ au mot (binaire)

(2) $b1b2 \ldots b_n$ dans $\{0; 1\}^*$

Alors la fonction de hachage (2), elle envoie le mot 01101 en (1). De façon plus générale, elle change une chaine de caractères b en 1 si le nombre de 1 dans b est impair (et sinon en 0) [25].

2.2.2.3 **Certificats numériques:** Il est essentiel d'utiliser une identité robuste, unique et immuable pour vos appareils dans une infrastructure à clé publique (PKI) ou une sécurité IdO basée sur la PKI. L'Autorité de Certification de confiance utilisée par GlobalSign émet le certificat numérique, qui est parfois appelé certificat de sécurité, certificat spécifique à un appareil, certificat d'appareil ou certificat PKI (CA). Il accorde les informations d'identification publiques et/ou privées nécessaires pour protéger le dispositif et lie une clé publique et privée pour lui donner une identité distincte [26].

Utilisé pour vérifier l'identité des parties dans les communications en ligne. Il existe pas mal de protocoles de sécurité tels que SSL/TLS/ DTLS, utilisé pour garantir la sécurité et l'intégrité des communications Internet.

Par exemple : Sur Internet, TLS (Transport Layer Security) [27] est le protocole de sécurité le plus souvent utilisé. Il établir une connexion sûre entre un client et un serveur web et utilise des protocoles de transport réputés, comme TCP.

Pour ce faire, TLS fait appel à deux niveaux : TLS Record et TLS Handshake.

TLS Record garantit la sécurité de la connexion entre le client et le serveur, grâce à des méthodes de cryptage comme DES. Le client et le serveur web négocient le jeu de clés et les méthodes de sécurité à utiliser pendant la phase TLS Handshake. Les messages ClientKeyExchange, ServerHello et ClientHello sont échangés pendant la négociation.

L'application de TLS aux réseaux de capteurs, qui utilisent fréquemment le protocole UDP dans la couche de transport, présente un défi important que certaines solutions ont tenté de relever. Bien que TLS soit efficace pour répondre aux exigences de sécurité, il implique des opérations cryptographiques asymétriques qui sont coûteuses en termes de temps de calcul et d'énergie.

2.2.2.4 **Authentification à deux facteurs :** Utilisé pour renforcer l'authentification en exigeant deux moyens différents d'identifier l'utilisateur, tels que par mot de passe et par code envoyé sur un téléphone mobile.

Pour les dispositifs IdO, la méthode d'authentification à deux facteurs (2FA) peut fonctionner de différentes manières. Pour vérifier l'identité de l'utilisateur, par exemple, un code envoyé à un téléphone mobile peut être utilisé comme second facteur ou un mot de passe établir. Cependant, une clé de sécurité physique peut être utilisée pour une interface utilisateur pour les dispositifs IdO qui n'en ont pas. Les clés de sécurité physiques sont utiles pour l'authentification à deux facteurs dans l'IdO car elles peuvent être utilisées pour confirmer l'identité des dispositifs eux-mêmes. Il est possible d'intégrer des clés de sécurité dans les dispositifs IdO pour fournir une authentification sécurisée des dispositifs vers les services en nuage. Cette approche est particulièrement utile pour les appareils IdO qui collectent des données sensibles ou gèrent des systèmes critiques.

2.3 **NIVEAUX DE L'IdO**

Avec des appareils connectés dans nos maisons, nos voitures et nos corps, L'IdO est de plus en plus présent dans notre vie quotidienne. Cependant, parce qu'elle crée un réseau d'appareils connectés qui pourraient être vulnérables aux cyber-attaques, cette technologie soulève des problèmes de sécurité. Afin de lutter contre ces dangers, il convient de prendre en compte la sécurité de l'internet des objets à chaque étape, de la perception à l'application.

2.3.1 **Le premier niveau est la couche perception**

Constituée d'éléments physiques du système IdO qui recueillent toutes sortes d'informations. Ce niveau permet d'améliorer la sécurité avec la garantie de la confidentialité et de l'authentification des informations échangées entre les nœuds [28] [29] aussi l'intégrité et la disponibilité des données collectées.

2.3.2 **Le deuxième niveau est la couche réseau**

Qui permet la communication entre les appareils IdO. Est responsable de la transmission des données obtenues par la couche de perception. À ce niveau, les mécanismes de sécurité existants tels que l'authentification, la confidentialité et l'exhaustivité des données, aussi garantir la disponibilité du réseau.

2.3.3 **Le troisième niveau est la couche de support**

Qui nécessite une sécurité élevée des applications, telles que le cloud computing et l'informatique multipartite sécurisée. L'informatique en nuage et l'informatique multipartite sécurisée, les algorithmes et de protocoles de chiffrement, technologies de sécurité des systèmes améliorées et antivirus... [28].

2.3.4 **Le niveau quatre, également appelé couche d'application**

Est chargé de donner du sens aux données collectées et transmises pour les besoins de l'entreprise. Des données collectées et transmises aux autres couches de l'IdO. Solutions de sécurité à ce niveau sont l'authentification et l'établissement d'une clé dans des réseaux hétérogènes. Cette dernière doit assurer la sécurité des données des utilisateurs et des applications en mettant en œuvre des protocoles de sécurité tels que le contrôle d'accès, la gestion des vulnérabilités et les mesures correctives [29].

En conclusion, la sécurité de l'Internet des objets est cruciale à la sauvegarde des données des utilisateurs et des entreprises. Les quatre niveaux clés de sécurité – perception – réseau – support – application, doivent être pris en considération pour y parvenir. Pour assurer la sécurité de l'Internet des objets et permettre son développement, des mesures de sécurité adaptées à chaque niveau doivent être mises en place.

2.4 **TYPES D'ATTAQUE**

L'IdO peut faire l'objet de multiples attaques. Dans cette section, nous allons présenter une liste non exhaustive d'attaques. Deux parties communiquant sur un canal non sécurisé, comme un utilisateur ou un appareil intelligent, ne sont pas considérées comme des entités de confiance. Un attaquant, dit A, peut écouter les messages échangés, mais aussi modifier ou supprimer le contenu des messages pendant la transmission [30] ; il est donc essentiel d'analyser toutes les attaques possibles contre l'IdO [31] :

2.4.1 L'attaque par relecture « rejeu »

L'attaque par relecture est également connue sous le nom d'attaque par lecture. Dans cette attaque, un adversaire intercepte les messages échangés pendant une longue période et les retransmet. Ces messages sont injectés dans le canal de transmission pendant l'authentification afin d'usurper l'identité du serveur ou de la passerelle. L'utilisation d'horodatages peut limiter l'effet de cette attaque contre les nœuds [32].

2.4.2 Attaque par écoute

Un adversaire écoute la communication échangée afin de capturer vos mots de passe, les détails de votre carte de crédit et les informations pendant la communication. Les données capturées peuvent également être utilisées pour connaître les protocoles de sécurité utilisés. Un cryptage symétrique avec une mise à jour périodique des clés peut empêcher ce type d'attaque.

2.4.3 Attaque par usurpation d'identité « Impersonation attack »

Dans cette attaque, un adversaire réussit à usurper l'identité de l'une des parties légitimes dans un canal de communication [33]. Par exemple, le nœud attaquant diffus de fausses informations de routage pour accéder aux données confidentielles des nœuds authentiques afin de devenir un nœud légitime sur le réseau.

2.4.4 Attaque de l'homme du milieu « MITM »

Ce type d'attaque est considéré comme une attaque en temps réel. Dans ce cas, un adversaire se place entre les parties qui communiquent et intercepte toutes les données échangées et les modifie ou les supprime en fonction de l'intention de l'attaquant. Cette attaque peut être exécutée pendant la phase d'authentification, ce qui peut permettre à l'attaquant d'avoir accès aux données et à toutes les communications futures. Dans un réseau conventionnel, l'utilisation d'un certificat numérique peut empêcher cette attaque (Voir la figure 2.1).

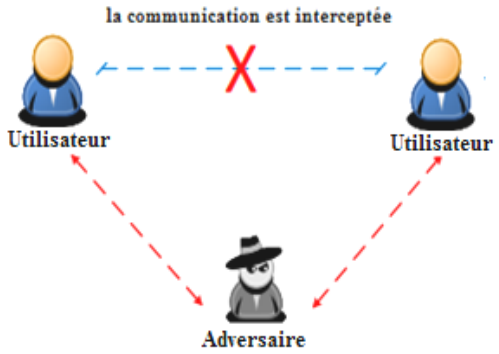

Fig 2.1. Attaque de MITM.

2.4.5 Attaque par déni de service

Cette attaque a pour but de consommer les ressources d'un nœud ou d'un serveur en lui faisant traiter des informations ou des demandes inutiles, dans d'autres cas, l'attaquant peut également cibler la bande passante du réseau afin d'arrêter ou de limiter l'accès à un serveur ou à une passerelle.

2.4.6 Attaque par dispositif intelligent volé « Stolen smart device attack »

Il s'agit d'une attaque visant à extraire les informations d'identification secrètes au moyen d'une attaque par analyse de puissance. Avec ces paramètres secrets, il est possible de connaître le mot de passe de l'utilisateur, et même la clé de session.

2.4.7 Attaque de session parallèle

Dans cette attaque, l'attaquant tente d'utiliser des messages précédemment piratés pour établir des sessions parallèles du protocole. Ou bien, l'attaquant peut réussir en utilisant deux ou plusieurs exécutions simultanées du protocole afin de contourner les objectifs de sécurité du protocole. Cette attaque se produit en l'absence d'un mécanisme d'authentification [34].

2.4.8 Attaque par changement de mot de passe

Pour cette attaque, un adversaire peut essayer de changer le mot de passe de l'utilisateur pendant la phase de changement de mot de passe, l'attaquant a accès au mot de passe et devient un utilisateur légal, ce qui rend un utilisateur légal incapable d'accéder au service [31].

2.4.9 Attaque de contournement du nœud de passerelle « Gateway node by passing attack »

En l'absence de tout protocole de sécurité, l'attaquant peut essayer de contourner le nœud de passerelle et se connecter directement à un nœud IdO sans être authentifié par le nœud de passerelle et accéder aux services ou aux données sensibles.

2.4.10 Attaque par devinette hors ligne

Dans cette attaque, un adversaire tente de deviner le mot de passe d'une entité légale en utilisant une attaque par dictionnaire hors ligne ou une attaque par force brute pour prendre le contrôle du système [31].

2.4.11 L'attaque par dictionnaire

Cette attaque a pour but d'essayer d'atteindre une liste ciblée de mots de passe faibles. En d'autres termes, l'attaquant essaie un nombre limité de combinaisons de clés qui ont de grandes chances de réussir à atteindre le vrai mot de passe.

2.4.12 **Attaque d'initié**

Un attaquant obtient l'accès à un réseau ou à un ordinateur et avec un privilège légitime afin d'avoir accès aux informations d'un utilisateur, comme les identifiants et les mots de passe.

2.4.13 **Attaque par compromission de nœud**

Il s'agit de l'une des attaques les plus courantes et les plus dommageables pour les réseaux WSN et IdO, où l'attaquant peut essayer de pénétrer dans les nœuds avec l'intention de d'extraire des données utiles (extraction de clés privées de nœuds de capteurs). Ces attaques peuvent obtenir le hachage du mot de passe utilisé comme complément pour l'attaque par devinette.

2.5 **AUTHENTIFICATION/PRIVACY DANS L'IdO**

Cette section résume les tâches liées aux protocoles d'authentification des utilisateurs:

2.5.1 **Protocoles D'authentification centralisée**

J. Jeong et al. [35] ont proposé un schéma d'authentification des utilisateurs basé sur le protocole de mot de passe à usage unique (OTP). Ce schéma est léger car il utilise une fonction de hachage unidirectionnelle. Cependant, l'authentification mutuelle entre les nœuds de passerelle (GWN) et les appareils intelligents n'est pas garantie. De plus, la véritable identité de l'utilisateur est transmise en clair, ainsi les propriétés d'anonymat et de traçabilité ne sont pas atteintes. En outre, le système est immunisé contre les cartes à puce volées et les attaques d'initiés privilégiés.

En 2009, Das et al. [36] a introduit une authentification d'utilisateur à deux facteurs dans le domaine des réseaux de capteurs sans fil en utilisant uniquement la fonction de hachage, qui ne fournit que l'authentification et la création de clés de session. Par la suite, les travaux de Khan et al. [37] et de Yeh et al. [38] en (2011) ont trouvé des faiblesses dans le schéma de Das et al, qui ne fournissait pas d'authentification mutuelle et était vulnérable aux attaques internes et aux attaques de contrefaçon. Plus tard, Shi et al. [39] ont présenté un protocole plus sûr et plus performant que le schéma de Yeh et al. Ensuite, Lee et al. [40] ont proposé un protocole amélioré pour les réseaux de capteurs sans fil en utilisant la cryptographie à courbes elliptiques. Ce dernier a souligné que le schéma de Yeh et al, ne fournissait ni une authentification mutuelle ni une confidentialité parfaite vers l'avant.

Le travail a également souligné que le schéma de Shi et al, était vulnérable à de nombreuses attaques connues telles que la clé de session, la carte à puce volée et l'épuisement de l'énergie du capteur.

Récemment, Hussain et al. [41] en 2021 ont introduit un protocole plus sécurisé en utilisant ECC. Le système utilise une nouvelle approche d'authentification mutuelle pour protéger les utilisateurs et les drones qui peuvent communiquer entre eux qui volent dans une région particulière, le schéma a été vérifié comme étant sûr contre les menaces connues.

En 2022, Min Zhang et al. [42] ont souligné que le système de Hussain et al. Présente certaines vulnérabilités : les attaques d'usurpation d'identité ne sont pas empêchées, ils montrent également comment un adversaire peut accéder à la clé de session d'un utilisateur cible et au drone qu'il a utilisé.

Au cours de la même année, Wu et al. [43] ont proposé un nouveau protocole d'authentification pour IoD sur 5G, le schéma résout le problème de sécurité de l'IoD, le schéma était sécurisé contre plusieurs attaques connues, le schéma proposé utilise la cryptographie symétrique avec des techniques de XOR et de hachage.

2.5.2 **Protocole d'authentification décentralisée**

Roman et al. [44] ont tenté de résoudre la sécurité IdO à travers diverses topologies IdO. Architecture centralisée et architecture distribuée. Encore une fois, ces solutions ne tiennent pas compte des ressources disponibles sur les appareils IdO, elles se concentrent uniquement sur la structure de haut niveau de ces topologies. D'autres recherches portent sur la communication sécurisée entre les appareils IdO.

Dans de nombreux articles récents, un mécanisme d'authentification décentralisé pour l'Internet des objets a été suggéré. Les auteurs Zhu et al. Ont proposé en 2019 un protocole d'authentification pour l'Internet des objets, basé sur la technologie des grands livres distribués (DLT) [45]. Ce protocole permet la gestion décentralisée des identifiants des objets et offre des méthodes de contrôle d'accès aux objets connectés.

Un protocole d'authentification décentralisé pour l'Internet des objets est également présenté dans l'étude " Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IdO Environment " de M. Zhaofeng et al [46]. La technologie Blockchain est utilisée par le système pour maintenir le secret et l'intégrité des données transmises entre les objets, ainsi que pour stocker et gérer les identités et les certificats des objets liés.

Un protocole d'authentification décentralisé basé sur des contrats intelligents est présenté dans l'article "A Decentralized and Distributed IdO Authentication Protocol Based on Smart Contracts" de Zhao et al. [47] en 2021. Pour garantir la sécurité et le secret des données transmises, le système permet l'administration décentralisée des identités et des autorisations des objets liés, ainsi que la vérification et l'exécution automatisées des smart contracts.

2.6 **LITTERATURE DES PROTOCOLES D'AUTHENTIFICATION**

Dans cette section, nous comparons, examinons et analysons les travaux les plus connus sur la sécurité de l'IdO (voir le Tableau 2.1).

- Muhamed Turkanovic et al [48]. Ils ont présenté un protocole d'authentification pour les WSN adapté à l'IdO. Le protocole fournit une authentification mutuelle entre l'utilisateur, le nœud capteur et le nœud passerelle (GWN).

  Ce protocole fournit une authentification mutuelle entre l'utilisateur, le nœud capteur et le nœud passerelle (GWN). L'équipe de recherche a fait le choix de calculs de hachage et

d'opérations XOR dans le protocole pour garantir sa légèreté, le système proposé protège contre diverses attaques populaires telles que les attaques par rejeu, les attaques d'initiés privilégiés, les attaques de vérificateurs volés, les attaques de violation de carte à puce, les attaques d'usurpation d'identité, les attaques d'utilisateurs multiples connectés avec le même identifiant de connexion, les attaques de contournement du GWN, les attaques de changement de mot de passe et les attaques par déni de service (DoS).

Les auteurs ont opté pour les avantages fondamentaux en matière de sécurité tels que l'établissement de clé dans l'IdO, l'authentification mutuelle et de l'anonymat de l'utilisateur pour concevoir leur protocole.

- Sur la base des faiblesses identifiées dans le protocole précédent [48], Mohammad Sabzinejad Farash et al [49]. Ont relevé certaines faiblesses dans la sécurité, qui le rendent sensible à diverses attaques cryptographiques. Conscients de ces lacunes, ils ont proposé un protocole amélioré pour l'authentification de l'utilisateur et l'établissement d'un accord de clé (UAKAS) au sein d'un réseau HWSN.

  Pour ce faire, ils ont intégré des mécanismes de calcul simples et peu coûteux tels que le XOR et le hachage. Toutefois, malgré ces améliorations, leur protocole présente encore certaines vulnérabilités qui compromettent sa sécurité.
- Dans ce protocole de Dhillon et al [31]. Proposent une méthode d'authentification multifactorielle de l'utilisateur qui s'avère être plus efficace en termes de calcul par rapport aux schémas précédents. Tels que, celui décrit dans [48].
- En 2018, Mohammad Wazid et al [50] ont présenté un schéma d'authentification à distance pour un réseau IdO hiérarchique appelé UAKMP (User Authentication Key Management Protocol), qui utilise une carte à puce légère avec trois facteurs : mot de passe, biométrie personnelle et analyse de diverses attaques connues, y compris l'exception de l'attaque de capture du nœud de capteur.
- Dans la même optique, Chen, Y et al [51] ont proposé un protocole léger basé sur des opérations XOR, des opérations de hachage et seulement quatre multiplications elliptiques, garantissant à la fois la protection de la vie privée et la sécurité des sessions. Leur protocole a été spécialement conçu pour les environnements IdO basés sur des appareils de faible capacité. Il offre des caractéristiques de sécurité telles que l'anonymat de l'utilisateur, l'anonymat du capteur et une excellente résistance au problème de la perte de synchronisation. En outre, la phase de changement de mot de passe a été modifiée pour empêcher les attaques de devinettes de mot de passe hors ligne et pour réduire les coûts de calcul et optimiser les coûts de communication.
- Un an après, Abderrezzak Sebbah et al [52] ont découvert que le protocole de Chen, Y et al [51] présente une certaine vulnérabilité face à diverses attaques. De plus, leur travail a proposé un schéma d'authentification à trois facteurs utilisant ECC et Fuzzy Extractor pour garantir une sécurité accrue contre différentes attaques.
- Récemment, Gupta, A et al [53] ont introduit un protocole assure la sécurité contre diverses attaques et se distingue par sa communication efficace et son coût de calcul réduit. Les auteurs de ce protocole ont introduit une méthode d'authentification légère et

d'établissement de clé pour les dispositifs portables en utilisant des opérations de XOR simple et une fonction de hachage.

- En 2019, Zhou, Y et ses collaborateurs [54] ont développé une capacité de dissociation pour l'environnement IdO afin de protéger la vie privée des utilisateurs et de prévenir des attaques telles que l'anonymat et d'autres attaques connues basées sur les paires bilinéaires.

Article	*Modèle de réseau*	*Objectifs*	*Resilience AGAINST & Limitations*	*Coûts de communication et de calcul*
[48]	La communication se fait entre l'utilisateur, le nœud de capteurs et le nœud passerelle GWN (entité de confiance).	-Accord de clés -Authentification mutuelle -Protection par mot de passe	-Replay attack -Privileged insider attack -Stolen-verifier attack -Stolen smart card -Smart card breach attack -Impersonation attack -GWN bypassing attack -Many logged-in users with the same login-id attack -Password change attack -Denial-of-service attack -User anonymity	Calcul : User=7TH Sensor=5TH GWN=7TH Communication:2720 bits
[49]	La communication se fait entre l'utilisateur, le nœud de capteurs et le nœud passerelle GWN (entité de confiance).	-Authentification mutuelle -Accord de clé de session -Modification du nœud dynamique	-Replay attack -Privileged-insider attack -Man-in-the-middle attack -Insider and stolen verifier attack -Smart card attack -User impersonation attack -Sensor node impersonation attack -GWN bypassing attack -Many logged-in users with the same login-id attack -Password change attack -DoS attack -Offline password attack -Traceability protection Password -User anonymity -Sensor node anonymity	Calcul: User=11TH Sensor=7TH GWN=14TH
[40]	La communication est de type USD. Si un utilisateur souhaite accéder à un nœud de détection correspondant à une application de l'IdO, il doit d'abord envoyer sa demande de connexion au GWN. Le GWN contacte ensuite le nœud de détection auquel il a accès via le cluster CH.	-Authentification mutuelle -Accord de clé de session -Détection rapide des entrées incorrectes	-User impersonation attack -GWN impersonation attack -Sensing device impersonation attack -Privileged-insider attack -Forward secrecy -Replay attack -Man-in-the-middle attack -Stolen verifier attack and smart card attack -Session specific temporary information attack -GWN bypassing attack -Sensing device capture attack -User anonymity -Sensor anonymity	Calcul: User=13TH+Tfe+2TE/TD Sensor=4TH+2TE/TD GWN=5TH+4TE/TD Communication: 2592bits

[41]	La communication se fait entre l'utilisateur, le nœud de capteurs et le nœud passerelle GWN (entité de confiance).	-Suivi de l'utilisateur -Proposition d'une authentification -Accord de clé de session	-Offline dictionary attack -Excellent resistance to the loss of synchronization problem -Perfect forward secrecy -User Anonymity -Sensor Anonymity -User Anonymity to sensor -Loss of synchronization -Protect the privacy of the data -Users being untraceable, -Sensors being untraceable	Calcul: User=5TH+TMUL Sensor=4TH+2TMUL GWN=8TH Communication: 396byte
[53]	Le modèle de réseau se compose de trois entités : le serveur, la passerelle/le terminal mobile et les dispositifs portables.	-Authentification mutuelle -Accord de clé de session	-Perfect forward secrecy -Replay attack -User impersonation attack -Sensing device impersonation attack -Gateway impersonation attack -Node capture attack -Offline guessing attack -Privileged insider attack -Man-in-the-middle attack -User anonymity -Sensor anonymity	Calcul: User=7TH+4TXOR Sensor=4TH+4TXOR GWN=5TH+3TXOR Communication: 3808bits
[54]	La communication se fait entre l'utilisateur, le nœud de capteurs et le nœud passerelle GWN (entité de confiance).	- Authentification mutuelle -Impossibilité de falsification des messages -Clé de session	-Unlink ability -Forward Security -Impersonation Attack -Replay Attack -Stolen Verifier Attack -Man-in-the-middle Attack	Communication: 1344bits

Tab 2.1. Comparaison des protocoles d'authentification dans L'IdO [55].

TH: Le temps d'une opération de hachage. TD/E: Le temps de décryptage/cryptage avec clés symétriques. TMAC: Le temps d'exécution de l'opération MAC. THMAC: le temps d'exécution de l'opération HMAC. TMUL: ECC multiplications. TXOR: Le temps pour l'opération XOR.

2.7 **CONCLUSION**

Dans ce chapitre, nous examinons en détail les objectifs et les fonctions de sécurité dans le cadre de l'internet des objets (IdO) et nous analysons la littérature sur les protocoles d'authentification utilisés dans ce domaine. Le principal objectif de cette étude est de mettre en évidence les enjeux de sécurité spécifiques liés à l'IdO, ainsi que les différentes approches et les différentes méthodes et les mécanismes existants pour relever ces défis. Cette analyse montre la diversité des protocoles d'authentification utilisés dans l'IdO, chacun ayant ses propres fonctionnalités et méthodes en matière de sécurité. Certains se focalisent plus particulièrement sur l'authentification mutuelle entre objets connectés, alors que d'autres soulignent des aspects spécifiques tels que la confidentialité des informations, l'intégrité des échanges ou la résistance aux attaques.

Pour synthétiser notre étude littéraire et pour faciliter la compréhension et la comparaison de ces protocoles, un tableau récapitulatif a été créé. Ce tableau offre une vue d'ensemble claire des différents protocoles d'authentification utilisés dans l'IdO, en soulignant leurs caractéristiques clés, les méthodes d'authentification utilisées, les types d'attaques qu'ils peuvent contrer, ainsi le coûts de communication et de calcul. Cet outil représente une précieuse ressource pour les chercheurs et les praticiens à choisir le protocole le plus adapté à leurs besoin spécifiques.

En particulier, il est essentiel de préciser que la sécurité des réseaux IdO est d'une importance primordiale. Les risques potentiels de piratage, les interceptions de données sensibles et la protection de la vie privée exigent une méthode d'authentification rigoureuse et dynamique.

CONTRIBUTIONS

- CHAPITRE 3: PROTOCOLE DE SECURITE PRESERVANT LA CONFIDENTIALITE POUR L'INTERNET DES OBJETS

- CHAPITRE 4: PROTOCOLE DE SECURITE AVANCE POUR LES ENVIRONNEMENTS IDO : UTILISATION ECC ET UN EXTRACTEUR FLOU

- CHAPITRE 5: AUTHENTIFICATION SECURISEE AVEC ECC POUR LA PROTECTION DE LA VIE PRIVEE DANS LES CONCEPTS IDO

Chapitre 3: Protocole De Sécurité Préservant La Confidentialité Pour l'Internet Des Objets

3.1 INTRODUCTION

L'infrastructure à clé publique (PKI) constitue la base des services sécurisés dans le domaine de l'Internet des objets (IdO), en particulier pour les services exigeant une garantie d'authenticité, de confidentialité et d'intégrité. La PKI établit le lien entre l'identité et la clé à l'aide de certificats. Ces certificats sont créés par une autorité de certification de confiance (AC) et signés par celle-ci. Cette signature permet de vérifier que le certificat est intègre, actuel et authentique [56].

La PKI assure la possibilité de suivre (la traçabilité) et la responsabilité lors de l'utilisation d'une paire de clés certifiée. Le certificat peut être mis à jour pour prolonger sa validité ou révoqué en le plaçant dans une liste de révocation. Il renferme des informations cruciales liées au propriétaire de la clé, prévenant ainsi toute tentative d'usurpation d'identité, ainsi que la période de validité et la clé publique. De plus, il contient des détails techniques tels que l'algorithme de signature numérique (DSA) employé, la fonction de hachage, la clé publique et l'identité du signataire. Ces données permettent au destinataire du certificat de vérifier la validité, l'authenticité et l'intégrité de la clé publique associée. Cette méthode est appelée "authentification basée sur les certificats". Une fois cette vérification effectuée et la clé acceptée, le propriétaire en assume la responsabilité pour toutes les communications sécurisées et les applications dans lesquelles elle est utilisée. Cependant, il est important de noter que l'activité de l'utilisateur utilisant cette clé certifiée est traçable. Bien que cette traçabilité soit un a tout en termes de sécurité, elle comporte des risques pour la vie privée, notamment dans les applications sensibles telles que les dossiers médicaux ou financiers. Révéler ou suivre des dossiers médicaux, des transactions financières ou la localisation des utilisateurs du réseau de véhicules peut entraîner des conséquences graves, telles que le chantage, la taxation ou la rétrogradation [56].

Dans le but de proposer une nouvelle approche garantissant la confidentialité, l'intégrité, l'authentification de l'utilisateur, ainsi que la protection de leur vie privée, nous avons introduit deux types de clés basées sur les courbes elliptiques (ECDH) : les clés certifiées à long terme, liées à l'identité, et les Alias anonymes temporaires, générés de manière dynamique. Ces Alias sont enregistrés de manière transparente par L'autorité de Certification qui maintient deux répertoires distincts pour les clés à long terme et les clés temporaires. Dans ce chapitre, nous concevons une PKI basée sur ECDH et travers une autorité de certification (CA (entité de confiance)) qui garantit la non-répudiation (responsabilité), l'intégrité et la fraîcheur, Cette PKI convient aux applications sensibles à la vie privée.

3.2 ANALYSE DES MENACES A LA VIE PRIVEE DANS L'IDO

Les attaques ciblant Privacy dans le domaine de l'Internet des objets (IdO) sont une source de préoccupation majeure, car elles ont le potentiel de compromettre la protection des données des utilisateurs et des dispositifs connectés. Voici une liste des attaques courantes qui menacent la vie privée dans l'IdO :

3.1.1 Attaques par interception de données (Eavesdropping) :

Une attaque (Eavesdropping) constitue une forme de cyber-attaque où les assaillants s'immiscent dans une conversation ou une transmission de données déjà en cours, que ce soit en écoutant de manière clandestine ou en se faisant passer pour un participant authentique. Les attaquants cherchent à intercepter les informations échangées entre les dispositifs IdO, exposant ainsi des données sensibles. Du point de vue de la victime, l'échange en cours semble être une communication normale, mais en s'insérant au "milieu" de la conversation ou de la transmission de données, l'attaquant peut subrepticement détourner des informations [57].

3.1.2 Attaques par analyse de trafic (Traffic Analysis) :

Les attaquants analysent les schémas de communication entre les dispositifs IdO, ou l'attaquant intercepte les messages échangés entre les parties communicantes, puis analyse attentivement ces messages pour déduire la nature et le contenu et les informations sur les activités des utilisateurs [57].

3.1.3 Attaques par usurpation d'identité (Identity Spoofing) :

Les attaquants se font passer pour des dispositifs IdO légitimes, leur permettant ainsi d'accéder à des données confidentielles ou de mener des attaques. Un nœud malveillant peut propager de fausses informations de routage dans le but d'accéder aux données confidentielles des nœuds authentiques et ainsi usurper leur légitimité au sein du réseau [58].

3.1.4 Attaques de localisation (Location Privacy) :

Les individus malveillants s'efforcent d'obtenir la localisation précise des dispositifs IdO ou de leurs utilisateurs, ce qui pourrait potentiellement révéler des informations sensibles ou confidentielles, compromettant ainsi la vie privée de ces derniers [56].

3.1.5 Attaques par déni de service (DoS) :

Le DDoS est réalisé par plusieurs attaquants dans le réseau en même temps. Certains exemples d'attaque DDoS sont les attaques par inondation qui consomment les ressources la bande passante du système ciblé. Les attaquants inondent les dispositifs IdO de trafic malveillant afin de les rendre inutilisables et mettant en péril la vie privée [59].

3.1.6 Attaques par corrélation de données (Data Correlation) :

Les assaillants agrègent des données provenant de différentes sources IdO dans le but d'obtenir une perspective plus holistique de la confidentialité d'un utilisateur [57].

3.3 TRAVAUX CONNEXES

La cryptographie à clé publique repose sur l'utilisation de deux types de clés distincts : une clé privée, qui doit être gardée secrète, et une clé publique, qui est accessible à tous les membres d'une communauté. Cette méthode assure la confidentialité, l'intégrité et l'authentification des données échangées. En général, la gestion de ces clés, y compris leur création, distribution, renouvellement et publication, est confiée à une Autorité de Certification (CA), formant ainsi une Infrastructure à Clé Publique (PKI) [60].

En matière de systèmes de sécurité, nous nous concentrons sur deux approches : l'ID-PKI et le CL-PKI. L'ID-PKI, ou Infrastructure à Clé Publique basée sur l'Identité, repose sur la méthode de la Cryptographie à Clé Publique basée sur l'Identité (ID-PKC) et évolue vers une Infrastructure à Clé Publique basée sur l'Identité (ID-PKI). Son objectif est de simplifier la gestion des certificats en utilisant les identités des utilisateurs comme clés publiques, ce qui permet de créer des liens étroits entre les individus et leurs certificats tout en réduisant les coûts de communication. Cependant, l'ID-PKI présente des inconvénients en raison de sa centralisation, notamment en ce qui concerne la génération des clés privées des individus, ce qui le rend moins adapté aux réseaux ouverts [61],[62].

Le CL-PKI, ou Infrastructure à Clé Publique sans Certificat, est une variante de l'IBE qui repose sur l'idée de la cryptographie sans certificat. Contrairement à l'IBE, le CL-PKI évite les problèmes d'escrow en se basant sur un tiers de confiance en possession d'une clé maître pour garantir la certification des clés publiques. Cela le positionne comme une solution intermédiaire entre l'AC traditionnelle basée sur des certificats et l'AC basée sur l'identité. Toutefois, le CL-PKI conserve une structure centralisée, ce qui peut entraîner des problèmes liés à la centralisation, comme mentionné précédemment [63].

L'infrastructure de clés publiques (PKI) pour l'Internet des objets (IdO) a pour objectif de garantir la sécurité des échanges entre les appareils IdO en leur attribuant des certificats. Ces certificats, notamment le certificat X.509, renferment des données sur le propriétaire de la clé, l'émetteur du certificat, sa période de validité, ainsi que des informations détaillées sur les algorithmes utilisés, le numéro de séquence du certificat et une signature numérique fournie par l'autorité de certification [64], [65].

Cependant, le schéma classique de la PKI s'appuie sur des Autorités de Certification (CA) qui jouent le rôle d'entités de confiance. Malheureusement, cette structure présente des faiblesses en termes de sécurité et de praticité, en particulier en cas d'attaque visant la Root-CA. Ces derniers temps, plusieurs incidents de sécurité ont mis en lumière ces vulnérabilités inhérentes à la centralisation [66].

Diverses initiatives ont cherché des alternatives, comme les PKI décentralisées sans Autorité de Certification (CA), qui cherchent à éliminer le besoin d'une tierce partie de confiance dans le système. Un exemple précurseur de cette approche est le concept de "Web of Trust," qui permet

l'échange de clés publiques sans recourir à une entité de confiance (CA). La technologie de la blockchain a suscité un grand intérêt depuis son introduction en 2008, et plusieurs travaux ont été proposés [67], [68]. Néanmoins, les dispositifs légers, tels que les Smartphones et les objets IdO, sont confrontés à des défis liés à la gestion de la blockchain en raison de leurs limitations de mémoire. À ce jour, aucune solution n'a entièrement résolu ce problème, et les recherches futures se concentreront sur la recherche de moyens pour permettre à ces dispositifs de fonctionner normalement tout en préservant leur vie privée.

Dans cette étude, nous présentons un système de PKI qui combine l'utilisation de l'ECDH (Elliptic Curve Diffie-Hellman) et utilise deux répertoires distincts pour les clés à long terme et à court terme par l'Autorité de Certification (CA). Cette approche offre une solution plus sécurisée et efficace pour gérer les certificats et les alias dans un environnement IdO. L'utilisation de l'ECDH garantit des communications sécurisées tout en réduisant la complexité des clés, tandis que la segmentation des répertoires permet une gestion plus précise des certificats à long terme et à court terme. Cette approche renforce la sécurité, la confidentialité et la flexibilité du système.

3.4 SECURITE DANS L'INTERNET DES OBJETS

L'Internet des objets (IdO) est utilisé dans divers secteurs, notamment les soins de santé, l'industrie, l'agriculture, et plus encore. Les appareils IdO communiquent principalement via des technologies sans fil, ce qui ouvre la porte à des menaces potentielles pour la sécurité des données échangées entre ces appareils et les smart-phones des utilisateurs. Les défis de sécurité sont particulièrement préoccupants pour les concepteurs de protocoles IdO, comme l'exemple d'une attaque réussie contre des dispositifs médicaux dans un hôpital en 2015 l'illustre [14 69].

Pour garantir la sécurité et l'efficacité des protocoles IdO, il est essentiel de prendre en compte les ressources limitées en termes de puissance de calcul de ces appareils.

3.4.1 PROPRIETES DE SECURITE

Pour sécuriser un réseau mobile, les objectifs de sécurité de base suivants doivent être atteints.

- **Confidentialité :** Les données doivent rester secrètes et ne peuvent être comprises que par les parties autorisées, empêchant ainsi tout accès, déchiffrement ou interception non autorisé.
- **Authentification :** Il s'agit de confirmer l'identité d'un utilisateur, d'un système ou d'une entité pour s'assurer de leur véritable identité déclarée, généralement par le biais de preuves telles que des identifiants, des mots de passe ou des empreintes digitales.
- **Intégrité :** Les données doivent rester inchangées, non corrompues et non altérées pendant leur stockage, leur transmission ou leur traitement, garantissant ainsi leur fiabilité.

- **Non répudiation :** Cette mesure vise à empêcher les parties impliquées de nier leur implication ou leur accord dans une transaction ou un accord, ce qui est essentiel pour prévenir les litiges ultérieurs.

3.4.2 Privacy (Protection de la Vie Privée)

La préservation de la vie privée est une question cruciale dans le domaine de l'internet des objets (IdO), en raison de la gestion de données sensibles à caractère personnel. Ces informations portent sur les données des utilisateurs concernés par cette technologie, y compris leurs actions, leurs activités, leurs habitudes et leurs interactions avec d'autres entités. De ce fait, la sécurité et la protection de ces données sensibles deviennent impératives, ce qui nécessite la mise en œuvre de moyens pour protéger les informations sur l'ensemble des dispositifs de l'IdO, des interfaces utilisateurs, ainsi que tout au long des phases de mémorisation, de communication et de traitements des informations.

Dans le but de protéger la confidentialité et la vie privée des personnes liées à ces appareils, directement ou indirectement, la notion de vie privée a été introduite. Elle peut être résumée comme suit :

- Le droit de l'utilisateur d'avoir un contrôle total sur les informations le concernant, avec la possibilité d'approuver ou de refuser leur divulgation.
- Le droit de l'utilisateur d'être certain que ses données ne seront utilisées qu'aux fins pour lesquelles il les a fournies.

Bien que la notion de vie privée ne fasse pas l'objet d'une définition universelle uniforme, son objectif principal reste la protection de toutes les informations liées à un utilisateur, qu'elles soient explicites ou déduites, contre toute divulgation, déduction, connaissance ou utilisation sans le consentement explicite de l'utilisateur. A titre d'exemple :

- **Paiement électronique :** les informations fournies par un utilisateur pour procéder à un versement électronique ne doivent pas être employées pour le tracer, contrôler ses activités ou découvrir ses habitudes d'achat sans son consentement.
- **Localisation et Traçabilité :** Lorsqu'un utilisateur autorise une application IdO à accéder à sa position géographique à des fins précises, il est essentiel de souligner que cette permission ne doit jamais être utilisée pour le tracer ou pour cibler la publicité sans son propre accord explicite.
- **Santé et Données Médicales :** Les Informations médicales rassemblées par les dispositifs IdO, tels que les moniteurs cardiaques ou les glucomètres, sont extrêmement sensibles. Dans ce contexte, il est essentiel que l'utilisateur conserve un contrôle absolu sur les personnes qui peuvent accéder à ces données et à quelles fins, qu'il s'agisse de professionnels de la santé, de chercheurs ou d'applications dédiées au suivi médical.
- **Domotique et Caméras de Sécurité :** Dans le cadre d'une maison connectée, les caméras de sécurité IdO sont conçues pour assurer la sécurité du domicile. Il est toutefois essentiel qu'elles ne soient pas utilisées pour surveiller la vie quotidienne des habitants sans leur autorisation.

- **Voitures Connectées :** Les Voitures connectés collectent un grand nombre de donnés, y compris les habitudes de conduite et la position géographique. Le contrôle de ces informations par l'utilisateur doit être total.

Dans le contexte de l'Internet des objets (IdO), des efforts considérables ont été déployés pour aborder la problématique de la vie privée [70], [71], [72]. Certaines de ces approches s'appuient sur des techniques cryptographiques, telles que l'anonymat ou le pseudo-anonymat (Alias), tandis que d'autres se concentrent davantage sur l'établissement de politiques ou de règles visant à garantir la confidentialité par le biais d'un processus de négociation entre le Client/le Serveur (fournisseur d'informations/consommateur d'informations). L'objectif de cet échange est de déterminer la quantité minimale d'informations à divulguer pour accéder au service souhaité.

3.5 **LES MECANISMES DE SECURITE**

3.5.1 **Public Key Infrastructure (PKI)**

Une Infrastructure de Gestion de Clés, couramment appelée Infrastructure à Clé Publique (PKI), désigne un ensemble intégré de technologies, de processus et de logiciels élaborés dans le but de garantir la gestion sécurisée des certificats numériques tout au long de leur cycle de vie. Les certificats numériques, ou certificats électroniques, revêtent une importance cruciale pour la sécurisation des transactions électroniques [73]. Ils facilitent la réalisation d'opérations cryptographiques, telles que le chiffrement et la signature numérique, fournissant ainsi des assurances essentielles : Confidentialité, Authentification, Intégrité, Non Répudiation…

Pour assurer ces objectifs la gestion de l'infrastructure PKI repose sur plusieurs entités essentielles qui sont intégrées dans l'ensemble du système PKI. Ces entités comprennent l'Autorité de Certification (AC), l'Autorité d'Enregistrement (AE), l'Autorité de Dépôt (Repository), et l'Entité Finale (EE). Chacune de ces entités remplit une fonction particulière dans la supervision des certificats et des clés [72].

- **L'Autorité de Certification (AC)** constitue une entité centrale de confiance qui occupe une position essentielle au sein d'une Infrastructure à Clé Publique (PKI). Son rôle majeur englobe la génération, la validation, et la signature numérique des certificats. En outre, elle détermine la politique de certification et établit des déclarations de pratiques de certification.
- **L'Autorité d'Enregistrement (AE)** a pour mission de vérifier l'identité des personnes physiques, morales, ou des équipements informatiques avant de soumettre une demande de certificat à l'AC.
- **L'Autorité de Dépôt (ou Repository)** Elle fonctionne comme un référentiel centralisé où les utilisateurs peuvent consulter et récupérer les certificats publics des autres entités de confiance. De plus, l'Autorité de Dépôt publie régulièrement des Listes de Révocation (CRL), répertoriant les certificats révoqués. Cela permet aux utilisateurs de vérifier la validité des certificats en circulation.

- **L'Entité Finale (EE)** L'EE utilise ce certificat pour réaliser diverses opérations cryptographiques, telles que le chiffrement des données ou la signature numérique.

La PKI trouve une grande utilité dans divers scénarios d'application, dont voici quelques exemples :

- L'utilisation de certificats SSL pour sécuriser les sites web et les services accessibles au grand public.
- L'application de la PKI dans des réseaux privés et (VPN) pour garantir des communications sécurisées.
- L'intégration de certificats numériques dans des applications et services hébergés sur des plates-formes de cloud public, assurant ainsi la protection des données.

Cependant, cette approche de la PKI présente des inconvénients liés à la nécessité d'autorités de certification, qui posent des problèmes de sécurité, convivialité et confidentialité, notamment en conservant la traçabilité de l'utilisateur, ce qui peut entraîner des risques pour la vie privée.

3.5.2 Elliptic curve cryptographie (ECC)

L'utilisation de courbes elliptiques en cryptographie a été proposée de manière indépendante en 1985 par Neal Koblitz [74] et Victor Miller [75].

Les courbes elliptiques utilisées dans ce contexte sont définies par une équation affine simplifiée de Weierstrass :

$E : y^2 = x^3 + ax + b$ (*)

Ces courbes elliptiques peuvent être représentées dans différents ensembles de nombres. En cryptographie, on les représente généralement dans des corps finis tels que Fp (où p est un nombre premier) et F2n.

Les coefficients a et b permettent d'identifier de manière unique une courbe elliptique. Les solutions de l'équation (*) sont des points Pi (xi, yi) appartenant à la courbe elliptique.

L'addition de deux points : L'addition de deux points de la courbe elliptique donne comme résultat un troisième point qui réside également sur cette courbe.

Une multiplication scalaire peut être définie en appliquant l'opération d'addition de points k fois. Cette opération est relativement simple à effectuer avec des nombres entiers, mais l'opération inverse, réalisée à l'aide de logarithmes discrets sur des nombres entiers, est computationnelle-ment difficile. C'est pourquoi la cryptographie à courbes elliptiques repose sur le Problème du Logarithme Discret (DLP) pour assurer sa sécurité.

Par exemple : L'opération

$S = k * P$ (**)

Représente l'addition du point P à lui-même k fois.

Si on exemple k=3

L'opération (**) devient $Q = 3 * P$ équivaut à $(2 * P) + P$, équivaut à $P + P + P$ [76].

Les courbes elliptiques offre une sécurité accrue par rapport à la taille de la clé utilisée, tout en étant particulièrement résistante à la régénération par des attaquants. En effet, contrairement aux méthodes de cryptographie conventionnelles comme RSA, où les clés

sont générées à partir d'opérations complexes, les clés ECC sont dérivées d'une ligne tracée sur une courbe elliptique. Par conséquent,

Une clé ECC= 256 bits peut offrir un niveau de sécurité équivalent à une clé RSA= 3072 bits.

Cette approche présente l'avantage de réduire l'espace de stockage requis et la bande passante nécessaire lors de la transmission des données [21 76].

3.5.3 **Elliptic Curve Diffie-Hellman (ECDH)**

Elliptic Curve de Diffie-Hellman est une variante de l'algorithme de Diffie-Hellman basée sur les courbes elliptiques. Il est très similaire à l'algorithme classique de Diffie-Hellman utilisé pour échanger des clés de manière sécurisée. Contrairement à Diffie-Hellman, qui effectue des opérations exponentielles sur les clés, l'ECDH utilise la multiplication de la cryptographie à courbes elliptiques [77], et s'avère un protocole finalement assez simple un exemple:

Pour illustrer le processus de l'ECDH, prenons un exemple concret :

Imaginons deux entités, désignées comme nœud A et nœud B, qui choisissent une courbe elliptique, un nombre premier P, et un point G (appelé Générateur) situé sur cette courbe.

- Le nœud A choisit un nombre aléatoire z-a qu'elle garde secret.
- En utilisant ce nombre, le nœud A calcule le point A= z-a * G et l'envoie au nœud B.
- À son tour, le nœud B choisit un nombre aléatoire, z-b, qu'il garde confidentiel.
- En utilisant ce nombre, le nœud B calcule le point B= z-b * G et l'envoie au nœud A.
- Le nœud A, et le nœud B effectue un calcul pour déterminer une secret partagé xk= z-a* B= z-a *z-b *G, De même, Le nœud B, xk= z-b* A= z-b* z-a* G.
- Le secret partagé obtenu par les deux parties est identique, car

z-a* B= z-a *z-b *G= z-b* A.

Cette méthode permet aux deux parties de calculer une clé partagée de manière sécurisée, même si des tiers essaient d'intercepter les échanges La Figure ci-dessus présente le principe du protocole ECDH.

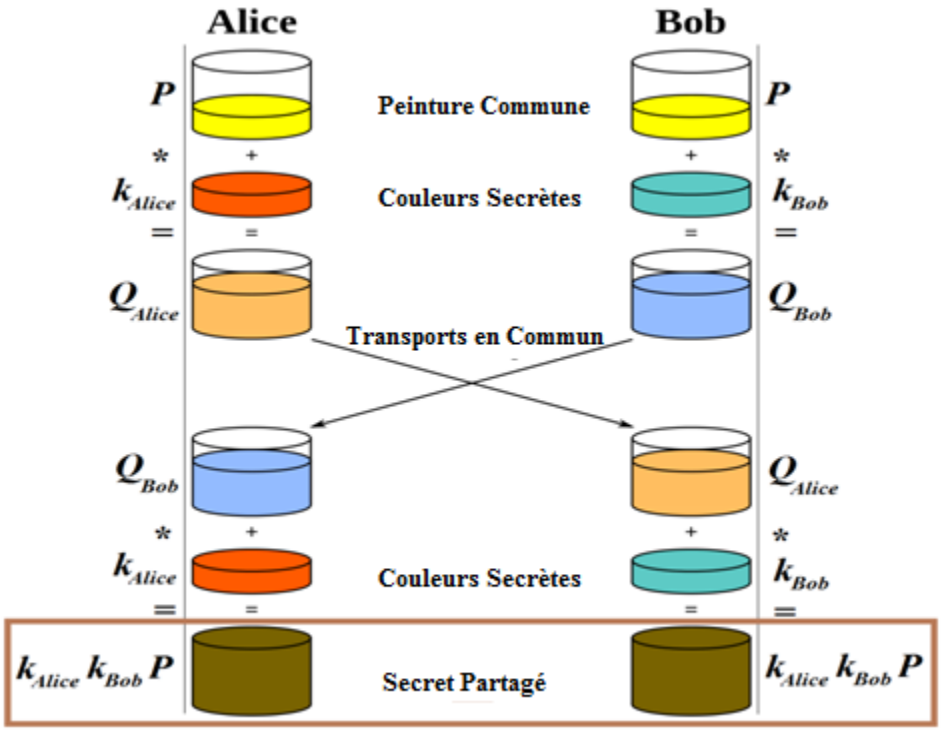

Fig 3.1. Principes fondamentaux du protocole ECDH [78].

3.6 **MOTIVATION**

La qualité d'un protocole de sécurité dépend de divers éléments, tels que le type de mécanisme de sécurité employé, la structure du réseau, et le contexte particulier de communication. Pour évaluer l'efficacité sécuritaire d'un protocole, il est impératif de tenir compte des spécificités inhérentes au réseau sur lequel il sera mis en œuvre.

- Le système de gestion de clés publiques (PKI) conventionnel basé sur l'autorité de certification (CA) présente diverses vulnérabilités. *En qui avons-nous confiance, et pour quoi ?* La question est de savoir si les informations fournies à la CA sont suffisantes pour lui faire confiance à l'utilisateur et certifier ses clés. La CA est une autorité dans la création de certificats, mais pas ailleurs donc sa donne de posé la question : *La CA est-elle une autorité ?*
- *Qui utilise ma clé ?* La non-répudiation rend le propriétaire de la clé responsable des activités effectuées avec cette clé.
- Ces vulnérabilités peuvent résulter d'une conception ou d'une mise en œuvre faibles de la PKI. L'un des principaux problèmes de la PKI actuelle est le problème du point de défaillance unique qui peut cibler la CA et perturber sa disponibilité. Ces vulnérabilités donne a posé la question : *Quelle est la sécurité des pratiques de certification ?*

3.6.1 **Supposition**

Dans ce chapitre, nous introduisons une proposition novatrice de PKI, qui repose sur l'utilisation de courbes elliptiques (ECDH) et PKI traditionnel afin de garantir la vie privée des utilisateurs. Les principales contributions de ce travail sont les suivantes :

1. Notre système repose sur des certificats anonymes, les Alias générer par l'utilisation d'un cryptage ECDH.
2. La PKI proposé basée sur deux répertoires distincts pour les certificats et les Alias Générer. Le premier répertoire contient les certificats (RCL), tandis que le second répertoire est réservé aux alias et contient liste de révocation (RRCT) qui est archivé.
3. Notre système sécurisé contre diverses attaques.

3.6.2 **Modèle de Réseau**

La figure 3.2 illustre le cheminement de la communication entre les différents éléments de l'internet des objets (IdO), en mettant l'accent sur la sécurité et la protection de la vie privée. Cette illustration présente un résumé visuel des communications sécurisées dans le cadre de l'IdO, tout en soulignant l'importance de la sécurité et de la protection de la vie privée. Elle explique comment les appareils de l'IdO peuvent échanger des informations en toute confiance sans compromettre la vie privée de l'utilisateur.

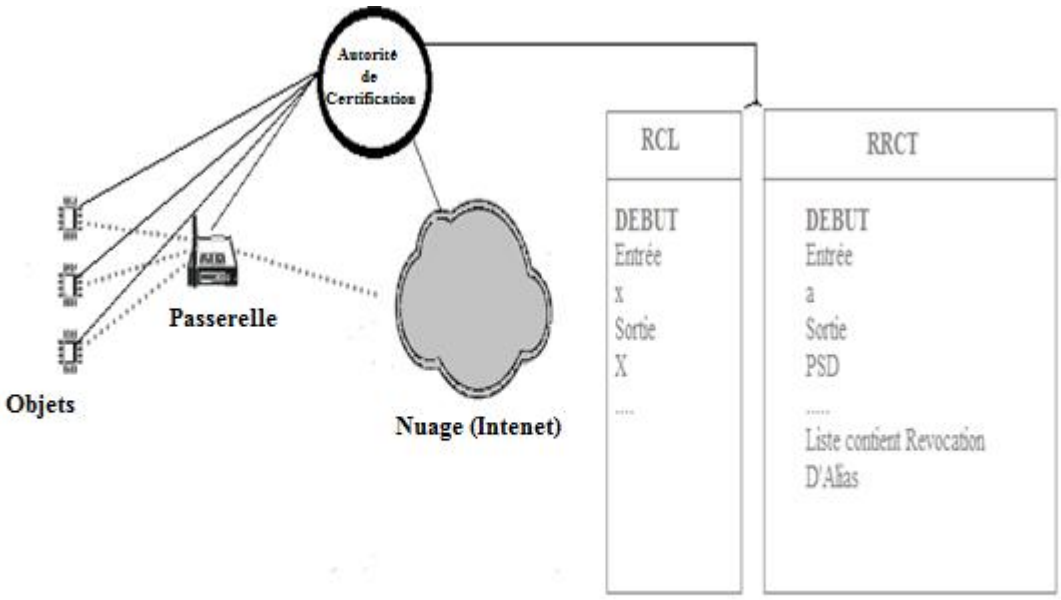

Fig 3.2. Modèle de réseau de notre protocole.

- **Objets de l'IdO :** Un certain nombre d'objets de l'IdO sont représentés sous forme d'icônes, divers dispositifs tels que des capteurs, des appareils domestiques, des véhicules connectés, etc. Ces objets interagissent entre eux pour échanger des données.

- **Passerelle IdO :** Au centre de la figure, des passerelles IdO sont positionnées pour faciliter la communication entre les objets IdO et l'extérieur du réseau. Les passerelles font office de points d'accès sécurisés.

- **Autorité de certification (CA) :** En haut du schéma, une icône représente l'autorité de certification (CA). L'autorité de certification est le point central de la sécurité dans l'écosystème de l'IdO.

- **Flux de communication :** Des flèches bidirectionnelles relient les objets IdO aux passerelles IdO, puis aux serveurs ou à l'Internet externe. Ces flèches symbolisent des échanges de données sécurisés.

3.7 LA SOLUTION PROPOSÉE

Dans cette section, nous présentons notre protocole qui repose sur une Elliptic curve cryptographie (ECC), et la PKI pour établit une association entre l'identité et la clé en utilisant des certificats. Ces certificats sont produits par une autorité de certification de confiance (CA) et validés par celle-ci. Cette validation permet de garantir l'intégrité, la fraîcheur, et l'authenticité des certificats.

L'Autorité de Certification maintient deux répertoires distincts pour les clés à long terme et les clés temporaires. Le premier répertoire contient les certificats (RCL), tandis que le second répertoire est réservé aux alias et contient liste de révocation (RRCT), qui sont utilisées pour la certification des clés à court terme, également connues sous le nom d'alias. Les deux répertoires sont archivés par l'autorité de certification, assurant ainsi une gestion sécurisée et traçable des clés utilisées dans le processus de certification.

Le modèle de réseau suggéré se compose de trois phases : Pré-déploiement, génération d'alias, Révocation d'Alias, el Vérification d'alias. Ces phases permettent d'atteindre une authentification entre l'utilisateur et Autorité de certification. (L'Algorithme 1 résume toute ces étapes).

Etape 1 : Pré-déploiement

- Un dispositif IdO doit établir une communication sécurisée avec un utilisateur autorisé. Le dispositif IdO génère une paire de clés ECDH :
    1. Clé privée du dispositif IdO (dev)

2. Clé publique du dispositif IdO (DEV = dev * P)

- ***Inscription initiale :*** Lorsqu'un utilisateur souhaite s'inscrire auprès de l'Autorité de Certification (CA), il fournit ses informations d'identité. Ces informations, présumées authentiques et suffisantes pour identifier l'utilisateur, sont utilisées par la CA pour délivrer un certificat à l'utilisateur.
- ***Certificat à long terme :*** Le certificat à long terme comprend deux paires de clés secrètes/publiques, notées (x, X), où x ∈ Z*n et X = x * P. Ces clés sont utilisées pour assurer la sécurité des communications.

Etape 2 : Génération de l'Alias

- ***Demande de l'alias :*** Lorsque l'utilisateur a besoin d'un alias (pseudonyme), il envoie une demande sécurisée à la CA. Cette demande doit inclure le certificat à long terme de l'utilisateur, contenant la clé publique X.
- ***Vérification de la révocation :*** La CA commence par vérifier si l'utilisateur demandeur n'a pas été révoqué, c'est-à-dire si X n'est pas dans la liste de révocation (CRL) maintenue par la CA.
- ***Génération de l'Alias :*** Si l'utilisateur est autorisé à obtenir un pseudonyme, la CA génère un nombre aléatoire a.
- ***Calcul de l'Alias :*** La CA génère ensuite l'alias PSD pour l'utilisateur en utilisant a et X de la manière suivante :
    1. PSD = a * X
    2. Remarque : Le PSD est une clé publique. De plus, seul l'utilisateur peut calculer la clé privée correspondante.
- ***Publication de l'Alias :*** La CA publie le PSD généré, sa période de validité et le nombre aléatoire a dans un répertoire réservé pour les clés temporaires (RRCT). Cette publication permet à l'utilisateur de rechercher son alias demandé dans ce répertoire (RRCT).
- ***Sauvegarde sécurisée :*** La CA sauvegarde de manière sécurisée le PSD généré et le certificat contenant la clé X. Cela garantit la traçabilité et la révocation en cas de comportement malveillant.
- ***Obtention de la clé privée correspondante :*** Pour obtenir la clé privée (x-z) correspondant au PSD généré, l'utilisateur effectue le calcul suivant :

  $$PSD = a * X$$

  Le secret partagé calculé par les deux parties est identique, car :

  $$a * X = a * x * P = a * X$$

  En effet, seul l'utilisateur peut déterminer la clé confidentielle x-z à partir du PSD et de a publiés, car il est le seul à pouvoir connaître la valeur de x.

ETAPE 3 : Révocation d'Alias par l'Autorité de Certification (CA)

- ***Révocation d'Alias :*** Pour révoquer un alias, l'Autorité de Certification (CA) utilise le PSD reçu dans le message de signalement de comportement malveillant.

- ***Recherche du PSD révoqué :*** La CA recherche le PSD signalé pour obtenir sa correspondance avec X. Pour faciliter la recherche et la rendre efficace, la CA se base sur la période de validité pour rechercher uniquement dans les blocs créés pendant la période de validité du PSD.
- ***Insertion dans la liste de révocation (CRL) :*** Lorsque la CA trouve X, elle insère leur certificat correspondant dans sa liste de révocation (CRL). Cette action empêche l'utilisateur de demander d'autres Alias à l'avenir.
- ***Partage de la CRL :*** La CRL est partagée entre les (CA) qui forment et maintiennent le RRCT. Elle est échangée de manière sécurisée entre elles.

ETAPE 4 : Vérification d'Alias :

Avant d'accepter un alias, le nœud récepteur doit effectuer les tests suivants :

- Vérifier le PSD dans la le répertoire réservé pour les clés temporaires(RRCT).
- Vérifier la période de validité du PSD.
- Vérifier le PSD dans la liste de révocation des transactions (CRL).

ETAPE 5 : Authentification avec dispositifs IdO

- ***Échange de Clés ECDH :*** Le dispositif IdO a l'intention de transmettre des données de manière sécurisée à l'utilisateur. Dans cette démarche, il acquiert le certificat de l'utilisateur (PSD), qui renferme la clé publique de ce dernier. Le dispositif IdO met en œuvre la méthode ECDH afin de créer une clé de session partagée (K-S) en utilisant la clé publique de l'utilisateur :

$$K\text{-}S = ECDH(dev, PSD) = dev*PSD = dev* a* X = dev* (a* x) = x\text{-}z* P$$

- ***Communication Sécurisée :*** Le dispositif IdO chiffre les données à envoyer à l'utilisateur avec la clé de session K-S et envoie les données chiffrées à l'utilisateur.
- ***Réception et Déchiffrement :*** L'utilisateur légitime obtient les données chiffrées du dispositif IdO. L'utilisateur emploie la méthode ECDH pour créer une clé de session partagée identique (K-S). Cette clé est générée à partir de sa propre clé privée (a-z) et de la clé publique du dispositif IdO (DEV) incluse dans le certificat du dispositif IdO :

$$K\text{-}S = ECDH(a\text{-}z, DEV) = a\text{-}z * dev * P = (a* x) = x\text{-}z* dev* P$$

L'Algorithme 1 : Le processus d'alias

```
    # Génération d'alias
1.  fonction generer_Alias (User):
2.  Si User non révoqué:
3.  a = genererNombreAleatoire ()
4.  PSD = a * User.cléPublique(X)
5.  Publier Dans(RRCT) (PSD, validité, a)
6.  sauvegarderPSDetCertificat (PSD, User.cléPublique)
7.  retourner PSD
8.  Fin
    # Révocation d'Alias
9.  fonction revoquer Alias (PSD_signalé):
10. X = trouver X à Partir De PSD (PSD_signalé, périodeValidité)
11. Ajouter X à CRL(X)
    # Vérification d'Alias
12. fonction verifier Alias (PSD):
13. Si PSD existe dans la (RRCT):
14. Si périodeValidité est valide:
    Si PSD non présent dans la liste de révocation:
    AccepterAlias ()
    « Authentification terminée avec succès »
    Sinon:
    RejeterAlias ()
    « Authentification échoue »
    Fin Sinon.
    « Authentification échoue »
    Fin.
    « Authentification échoue »
    Fin.
    # Authentification avec dispositifs IdO
    Def authentification_IdO (dev_private_key, PSD):
       K_S = ECDH (dev, PSD)
       Donnees_chif = chiffrement (K_S, Inf_a_envoyer)
       Envoyer_donnees_chiffrees (Donnees_chif)
```

3.8 **ANALYSE DE SÉCURITÉ**

Cette partie procède à une évaluation approfondie de la sécurité de la conception du protocole proposé en se basant sur les différents types d'attaques sur les dispositifs IdO émergents. La solution proposée garantit plusieurs caractéristiques de sécurité, notamment :

- **Concept de la vie privé (Privacy)** Chaque composant de la requête de connexion varie de manière dynamique en utilisant un nombre aléatoire a. Ainsi, lorsqu'un attaquant intercepte les demandes de connexion, il est impossible de tracer un utilisateur particulier, assurant ainsi la préservation de l'anonymat. Notre approche garantit une confidentialité totale. Les clés temporaires (alias) enregistrées dans la Répertoire sont dépourvues d'informations d'identification (anonymes). Les données personnelles de l'utilisateur incluses dans le certificat à long terme contenant 'X' sont échangées de manière sécurisée avec l'Autorité de Certification lors de la demande d'alias.
- **Authentification mutuelle :** Chaque étape du système proposé dispose d'une autorisation spécifique, basée sur une clé secrète partagée lors de la phase vérification d'Alias. L'utilisateur Ui et le CA s'authentifient mutuellement, et établissent une clé de session privée en utilisant PSD, a, tout en vérifiant éléments suivants :
  PSD = a * X
  Le secret partagé calculé par les deux parties est identique, car :
  a * X = a * x * P = a * X
  Le protocole proposé assure une authentification mutuelle.
- **L'intégrité** Les Alias sont générés par l'autorité de certification (AC) à l'aide d'un nombre aléatoire et de la clé publique du propriétaire. Une fois qu'un pseudonyme est généré, il est consigné dans les répertoires, ce qui assure son intégrité. Toute tentative de modification ou d'altération du pseudonyme serait immédiatement détectée. Par conséquent, les Alias bénéficient de l'intégrité grâce à leur enregistrement public et immuable.
- **La non-répudiation** Dans le contexte des Alias, une fois qu'un pseudonyme est enregistré, son propriétaire ne peut pas le réfuter ou nier qu'il en est le créateur ou le détenteur. Ceci est en parfait alignement avec le principe de l'intégrité des données stockées dans le répertoire.
- **Fraîcheur** Les transactions d'Alias trouvée dans les Répertoires de l'autorité de certifications sont dotées de horodatages et de périodes de validité spécifiques grâce à le nombre aléatoire a.

Notre approche est également capable de résister aux types d'attaques suivants :

- **Contre les attaques de rejeu** Le protocole assure sa sécurité grâce à l'utilisation d'une technique de numérotation aléatoire. Chaque utilisateur Ui et l'Autorité de Certification (CA) génèrent des valeurs aléatoires x, a. L'incorporation de ces valeurs aléatoires garantit que les messages étendus restent constamment à jour et récents, ce qui prévient les attaques de rejeu.
- **Une attaque par déni de service distribué DDoS** Pour attaquer la disponibilité de la PKI basée sur les répertoires et la paralyser, tous les nœuds doivent être attaqués en même temps.

Pour illustrer l'idée selon laquelle tous les nœuds doivent être attaqués en même temps, voici un exemple simplifié :

Imaginez un groupe de personnes qui dépendent d'une bibliothèque virtuelle partagée sur un réseau de cloud computing pour accéder à leurs livres électroniques. Chaque personne peut télécharger ces livres depuis n'importe quel nœud du réseau pour les lire.

Dans ce scenario:

Les nœuds du réseau cloud représentent les serveurs où la bibliothèque virtuelle est stockée.

Les utilisateurs du réseau sont les personnes qui souhaitent lire les livres électroniques. Maintenant, considérons qu'un groupe malveillant souhaite perturber l'accès à la bibliothèque virtuelle. Pour ce faire, ils décident de mener une attaque par déni de service distribué (DDoS).

Maintenant, si le groupe malveillant coordonne son attaque de manière à ce que tous les membres attaquent tous les serveurs en même temps, alors tous les serveurs deviennent inaccessibles simultanément. Les utilisateurs ne peuvent plus accéder à leurs livres électroniques, car l'ensemble du service est paralysé. C'est l'équivalent de ce qui serait nécessaire pour paralyser la PKI basée sur des répertoires.

- **Confidentialité à Avancement (Forward secrecy)** Supposons qu'un assaillant tente de compromettre les paramètres à long terme des entités actives, notamment les clés privées et publiques d'une étiquette et d'un lecteur. Pour créer une clé de session, nous utilisons le PSD et X. Ces paramètres (PSD et X) sont générés à l'aide de deux nombres aléatoires, x et a.

  Même si un assaillant parvient à s'emparer de la clé privée de l'entité, il reste incapable de calculer la clé de session grâce aux théorèmes ECDHP. En conséquence, il demeure incapable de générer la clé de session.
- **Une attaque de vérification des clés volées (Stolen Verfy Attacks)** Imaginons

  Qu'un attaquant tente de réaliser une attaque de vérification des clés volées (Stolen Verify Attack) en cherchant à accéder aux paramètres à long terme des entités actives, tels que les clés privées et publiques. Pour générer une clé de session, nous utilisons le PSD= a * X (Pseudo-Shared Secret) et X= x * P. Ces paramètres (PSD et X) sont créés à l'aide de deux nombres aléatoires, x et a.

  Les théorèmes de Diffie-Hellman sur les courbes elliptiques garantissent que même si l'attaquant obtient la clé publique d'une entité, qui est X dans notre cas, et la clé privée d'une autre entité, qui pourrait être la clé privée de l'étiquette ou du lecteur, il ne peut pas calculer la clé de session. Cela signifie que l'attaquant ne peut pas interagir avec le système de manière frauduleuse, car il ne peut pas générer la clé de session nécessaire pour établir une communication sécurisée.
- **Impersonation:** Supposons qu'un attaquant enregistre une de ces demandes dans le but de l'utiliser ultérieurement. Dans ce cas, l'autorité de certification génère des

alias temporaires en utilisant la clé publique du certificat. Par conséquent, seuls les propriétaires légitimes de ces alias détiennent les clés privées correspondantes, ce qui rend impossible pour l'usurpateur de déchiffrer des données cryptées avec ces alias ou de les utiliser pour signer des messages, étant donné que l'usurpateur n'a pas accès à ces informations sensibles.

Prenons un exemple où un attaquant $\tilde{A}$, souhaite usurper l'identité de l'utilisateur U et demander des alias au nom de U afin d'éviter d'être traçable. $\tilde{A}$ envoie une demande d'alias sécurisée contenant le Certificat U. Les autorités de certification génèrent l'alias PSD et l'insèrent dans le répertoire aux côtés de a-new.

PSD = X * a-new. $\tilde{A}$ récupère PSD à partir de le répertoire, mais, pour pouvoir l'utiliser, $\tilde{A}$ doit être en mesure de calculer x-z, la paire de clés privées de PSD, x-z = x * a-new. Étant donné que x est la clé privée uniquement connue de l'utilisateur U, l'attaquant $\tilde{A}$ ne peut pas usurper l'identité de U.

3.9 **CONCLUSION**

Ce chapitre, présente une proposition novatrice de PKI (Infrastructure à Clé Publique) basée sur deux répertoires RRCT/RCL. Notre approche combine habilement les principes d'une PKI traditionnelle avec ECDH afin de garantir la confidentialité des utilisateurs. Notre système repose sur des certificats anonymes, que nous appelons Alias ou pseudonymes. Ces pseudonymes sont générés à partir de la clé publique d'origine à l'aide de l'algorithme ECC (Elliptic Curve Cryptography), établissant ainsi une liaison entre l'identité réelle des utilisateurs et leurs pseudonymes. L'une des caractéristiques essentielles de notre approche est qu'aucune autorité légitime ne peut révéler l'identité réelle d'un utilisateur à partir de son pseudonyme, garantissant ainsi un niveau élevé de confidentialité.

Afin de renforcer la sécurité et la résistance de notre approche, nous avons pris des mesures pour minimiser les vulnérabilités liées à un point unique de défaillance, à différentes attaques populaire. Cette conception robuste et résiliente est basée sur une architecture légère, ce qui la rend appropriée pour un large éventail d'applications.

CHAPITRE 4: PROTOCOLE DE SECURITE AVANCE POUR LES ENVIRONNEMENTS IDO : UTILISATION ECC ET UN EXTRACTEUR FLOU

4.1 **INTRODUCTION**

Les appareils connectés et les échanges des données via l'internet peuvent être vulnérables aux attaques de hackers. Ils ouvrent un horizon négatif de problèmes de sécurité et de confidentialité qui doivent être traités délicatement avant le déploiement de tout IdO.

Par exemple, L'attaque du botnet Mirai en 2016, qui a utilisé des appareils IdO compromis pour mener une attaque massive par déni de service distribué (DDoS) contre le fournisseur de services de DNS Dyn, provoquant la mise hors ligne de sites Web populaires tels que Twitter, Reddit et Netflix [79] donc il est essentiel de mettre en œuvre des dispositifs de sécurité appropriés dans l'IdO implique l'utilisation de diverses mesures pour minimiser la vulnérabilité d'un système face aux risques tant accidentels qu'intentionnels.

Des initiatives de recherche récentes ont proposé des solutions d'authentification pour répondre à ces défis. Par exemple, Yuwen Chen et al [51] ont présenté un schéma d'authentification d'utilisateur pour l'IdO. Ils ont analysé l'anonymat des utilisateurs, l'anonymat des capteurs, et l'impossibilité de tracer les utilisateurs dans ce scénario, mais ont constaté certains inconvénients contre diverses attaques telles que les attaques internes et les attaques de vol de carte intelligente. En 2017, Xiong Li et al [80] ont discuté des problèmes de sécurité de l'Internet industriel des objets et ont présenté la confidentialité et l'authentification des utilisateurs en utilisant ECC. Le schéma proposé est sécurisé contre diverses attaques. La même année, Saru Kumari et al [50] ont présenté un schéma d'authentification d'utilisateur utilisant ECC qui assure l'anonymat des utilisateurs et est sécurisé contre diverses attaques. Ils ont également analysé la revue et la cryptanalyse du schéma de Lu et al [81]. Un an plus tard, Xiong Li et al [82] ont introduit un schéma applicable aux WSN et à l'IdO qui utilise ECC et la liaison floue. Dés que Khwaja Jawad et al [83] ont souligné que Xiong Li et al [82] présentait des vulnérabilités et des lacunes telles que les attaques de vol de carte intelligente, l'anonymat et la traçabilité, et ont présenté un schéma à trois facteurs qui assure l'authentification anonyme.

Ce chapitre se concentre sur une analyse approfondie du protocole proposé par Yuwen et al. en matière de sécurité dans les environnements IdO. Une évaluation minutieuse révèle que ce protocole reste exposé à diverses vulnérabilités, notamment les attaques internes et celles impliquant le vol de cartes intelligentes, compromettant ainsi la robustesse du système et menaçant la confidentialité des données dans les contextes IdO.

En réponse à ces lacunes, une solution novatrice est présentée : un protocole d'authentification mutuelle et d'établissement de clé sécurisé spécialement conçu pour l'IdO. Ce dispositif s'appuie sur l'association d'un Extracteur Flou et du cryptage ECC. L'Extracteur Flou vise à dissocier de manière irréversible les informations sensibles des identifiants spécifiques, empêchant ainsi toute tentative de traçage ou de ré-identification non autorisée. Parallèlement, le cryptage ECC assure la confidentialité des données échangées en les protégeant contre toute forme de compromission ou d'interception non autorisée.

L'adoption de cette solution garantit aux utilisateurs et aux capteurs une infrastructure robuste et fiable pour la protection de leur identité et de leurs données sensibles. Les risques associés aux attaques potentielles, telles que les attaques internes ou celles exploitant le vol de cartes intelligentes, sont considérablement réduits. Ainsi, l'authentification mutuelle et l'établissement de clé sécurisé garantissent l'anonymat, l'impossibilité de traçage et la confidentialité des informations échangées dans les environnements IdO.

4.2 **PRELIMINAIRES**

Dans cette section, nous donnons les notations dans un tableau, puis nous présentons notre contribution après avoir présenté l'examen et la cryptanalyse des schémas de Yuwen et al.

4.2.1 **Hypothèses et Modèle du réseau**

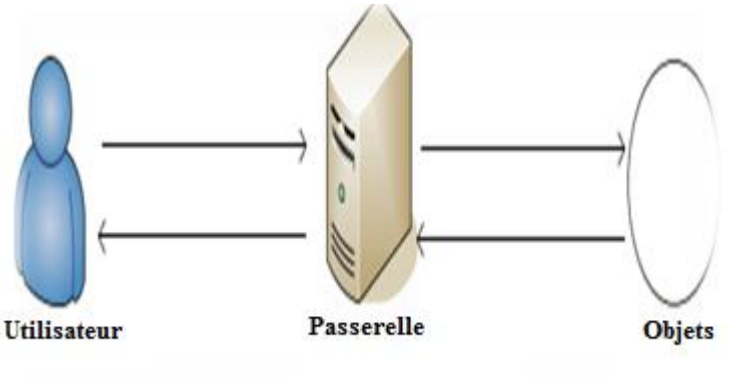

Fig 4.1. La structure du modèle [51].

La performance d'un protocole de sécurité dépend non seulement du mécanisme de sécurité utilisé, mais également de l'architecture du réseau et du scénario de communication. Pour évaluer la sécurité d'un protocole, il est important de prendre en compte les caractéristiques du réseau sur lequel il sera déployé. Dans notre cas, le réseau cible est composé de trois types de nœuds : les utilisateurs, la passerelle (GWN) et les dispositifs IdO, où la GWN doit être un membre de confiance et communiquer les données entre les capteurs (voir Figure 5.1).

Les solutions existantes, y compris celle que nous proposons, se composent de quatre phases : une phase d'enregistrement, une phase de Login et une phase d'authentification. Ces phases seront décrites plus en détail dans les sections suivantes.

La première phase est la phase d'enregistrement, où l'utilisateur (Ui) se trouve à proximité de la passerelle GWN. Pendant cette phase, l'utilisateur fournit ses informations d'identification et ses informations biométriques, qui sont ensuite stockées dans la carte à puce. Cette phase est effectuée une seule fois dans un endroit sécurisé

La deuxième phase est la phase de login, où l'utilisateur doit fournir ses informations d'identification et son empreinte biométrique pour être authentifié par le système.

Les figures 4.1 présentent l'architecture physique du réseau lors de la phase d'enregistrement et lors de la phase de login-authentification. La figure donnent une vue détaillée des différents composants et de leur positionnement dans le réseau.

4.2.2 **Notations**

Le Tableau 4.1, joue un rôle important dans le protocole proposé, car il répertorie toutes les notations utilisées. Il fournit une référence essentielle pour comprendre et interpréter les différentes variables, symboles et abréviations qui sont utilisés tout au long du protocole.

Symboles	Description
U_i, GWN	L'utilisateur et la passerelle.
Sj	Le dispositif de détection
SC	La carte à puce
IDu	L'identité de l'utilisateur
SIDj	L'identité du capteur
PWu	Le mot de passe de l'utilisateur
BIOu	La biométrie de l'utilisateur Ui
a, e, b, c	Nombres aléatoires
SKij, SKij‘	La clé secrète partagée entre Ui et GWN
XGWN	La clé de session de GWN
XGWN-U	La clé partagée entre Ui et GWN
XGWN-SD	La clé partagée entre SD et GWN
G	Le générateur de la courbe elliptique
A	Adversaire L'attaquant
h	La fonction de hachage
||	Connecte deux chaînes de caractères ensemble
$\oplus$	Opération XOR

Tab 4.1. Tableau des notations.

4.2.3 **Examen du protocole de Yuwen Chen et al**

Yuwen utilise un schéma d'authentification et d'établissement de clé pour l'IdO en utilisant les opérations XOR, les opérations de hachage et les multiplications elliptiques. Le schéma de Yuwen se compose de trois parties : les utilisateurs, la passerelle (GWN) et les dispositifs IdO, où la GWN doit être un membre de confiance et communiquer les données entre les capteurs (voir Figure II).Dans un premier temps, la passerelle sélectionne sa clé secrète XGWN et les paramètres (p, a, b, G, n et h) et la garde secrète de la même manière que le protocole de [Yuwen]. Ensuite, la passerelle publie (p, a, b, G, n et h) pour les utilisateurs sur le réseau. Le schéma de Yuwen Chen et al., est composé de trois phases : la configuration, l'enregistrement, l'authentification et l'établissement de clé.

A. Phase d'enregistrement des capteurs

Dans cette phase, chaque capteur doit s'enregistrer auprès de la passerelle pour rejoindre le réseau et obtenir les paramètres de sécurité nécessaires. Cette phase est réalisée en exécutant les étapes suivantes.

5 Étape 1 : Le nœud GWN sélectionne une identité SIDj pour chaque capteur et l'envoie au capteur via un canal privé.

6 Étape 2 : Le nœud GWN calcule le secret xj = h(SIDj || XGWN) et l'envoie au capteur Sj via un canal privé.

7 Étape 3 : Le capteur Sj stocke xj dans sa mémoire.

B. Phase d'enregistrement de l'utilisateur

Pour utiliser les services du réseau, un utilisateur doit être enregistré auprès de GWN comme suit :

- Étape 1 : L'utilisateur sélectionne IDi et PWi. Ensuite, l'utilisateur Ui produit un nonce aléatoire ri et calcule MPi = h(PWi || ri || IDi). Ensuite, Ui envoie la demande d'inscription {IDi, MPi} à la passerelle GWN via un canal privé.
- Étape 2 : Le nœud GWN calcule : di = h(IDi || XGWN); fi = di ⊕MPi; puis GWN choisit un nombre aléatoire ki et calcule : ei = h(ki || XGWN); li = ei ⊕ MPi; Ensuite, GWN envoie {fi, li, ki} à Ui via le canal privé.
- Étape 3 : Ui reçoit les paramètres de GWN et stocke ri et MPi dans la carte à puce (SC). La carte à puce contient les paramètres {fi, li, ki, MPi, ri}.

C. Connexion et authentification

Le processus d'authentification entre un utilisateur et un capteur doit être validé par GWN et doit suivre les étapes suivantes :

- Étape 1 : L'utilisateur Ui insère sa carte à puce dans un lecteur de carte et saisit son identifiant IDi' et son mot de passe PWi'. La carte à puce calcule MPi' = h(ri || IDi' || PWi') et vérifie si MPi' et MPi sont égaux. Ensuite, l'utilisateur calcule di = fi ⊕ MPi' et ei = li ⊕ MPi'. La carte à puce sélectionne ensuite un nombre aléatoire k1 ∈ [1, n – 1] et calcule : A = k1 • G, M2 = h (A || IDi || SIDj || di || T1), M1 = ei ⊕ (IDi || SIDj || M2). Pour terminer cette étape, l'utilisateur récupère le ki stocké et envoie {A, ki, M1, T1} à GWN via un canal ouvert.
- Étape 2 : Après la réception du message de l'utilisateur, GWN vérifie la fraîcheur de T1 : GWN calcule ei' = h(ki || XGWN) et déchiffre M1 en utilisant ei' pour obtenir (IDi' || SIDj || M2). GWN calcule également di' = h(IDi' || XGWN), xj' = h(SIDj' || XGWN) et vérifie si les paramètres M2' {di', A, IDi', SIDj', T1} sont égaux ou non au M2 reçu, sinon : GWN obtient T2, calcule M3 = h (A || SIDj' || xj' ||T2) et envoie à Sj {A, M3, T2}.
- Étape 3 : Lorsque Sj reçoit un message, il vérifie la fraîcheur de T2 ; et vérifie que M3 reçu de GWN n'est pas égal à l'authentification demandée. Sinon, Sj choisit un k2 aléatoire ∈ [1, n – 1] et calcule B = k2 • G et la clé de session partagée entre Ui et Sj :

SKij = h(k2 • A) = h(k1 • k2 • G). Ensuite, le capteur calcule M4 = h(B || SKij || A) et M5 = h(A || xj || M3 || M4 || B) et envoie {B, M4, M5} à GWN.

- Étape 4 : Chaque fois que GWN reçoit une demande de Sj, il vérifie si M5 = h(A || xj || M3 || M4 || B) et si le message reçu est égal. GWN choisit un k3 aléatoire, calcule einew = h(k3 || XGWN), M7 = h(einew || k3 || di' || T1 || M4) et M6 = (einew || k3 || M7) ⊕ ei' et envoie {B, M6} à Ui.
- Étape 5 : Ui reçoit la demande de GWN, récupère einew′ || k3′ || M7′ = M6 ⊕ ei. Ensuite, il calcule la clé de session partagée entre Ui et Sj : SKij′ = h (k1 • B) = h (k1 • k2 • G), et obtient M4′= h (B || SKij′ || A) et vérifie si M7 est égal pour accepter ou non SKij′. Enfin, Ui met à jour li = MPi′ ⊕ einew ′, ki = k3.

D. CRYPTANALYSE DU SCHÉMA DE YUWEN ET AL

Nous avons analysé le protocole de Yuwen et al. et avons constaté que leur protocole est encore vulnérable à diverses menaces et attaques de sécurité telles que les attaques d'initiés, les attaques de cartes à puce volées et l'anonymat.

a) **Attaque de carte à puce volée** Le schéma de Yuwen et al., est vulnérable aux attaques de cartes à puce volées ; lorsque l'utilisateur stocke certains paramètres dans la carte à puce lors de la phase d'inscription comme {fi, li, ki, MPi, ri}. Ainsi, la carte à puce volée par un adversaire $\mathcal{A}$ peut obtenir l'identité des utilisateurs et leur mot de passe en adoptant les étapes suivantes :
   - Étape 1 : Obtenir di' et ei' par : di' = fi ⊕ MPi et ei' = li ⊕ MPi.
   - Étape 2 : Deviner un XGWN*, calculer ei* = h(ki || XGWN*) et vérifier la condition ei* = ei. Si cela est vrai, le XGWN* supposé est correct, c'est-à-dire XGWN* = XGWN. Sinon, répéter en devinant une autre clé secrète GWN jusqu'à ce que $\mathcal{A}$ réussisse.
   - Étape 3 : A peut deviner l'IDi en utilisant les valeurs di' et XGWN' et le mot de passe PW par MPi lorsque l'adversaire a IDi' et ri et MPi.

b) **Attaque d'initié privilégié** Lors de la phase d'inscription, Ui envoie à la GWN à la fois IDi et PWi et ri via un canal sécurisé pour personnaliser la carte à puce. Un utilisateur privilégié à la GWN, en étant un attaquant interne, le mot de passe PWi est révélé à l'attaquant interne et a ainsi accès à ces informations secrètes de Ui. Ainsi, le schéma de Yuwen et al, ne parvient pas à se protéger contre les attaques d'initiés privilégiés.

4.3 LA SOLLUTION PROPOSÉE

Dans cette section, nous présentons notre protocole qui repose sur une forte ECC et un Fuzzy Extractor pour garantir l'anonymat de l'utilisateur/du capteur pour l'IdO et l'absence de traçabilité. Afin de pré-déployer le système, GWN génère une clé secrète XGWN connue uniquement par la passerelle et une clé partagée avec l'utilisateur XGWN-U et une clé partagée avec les capteurs XGWN-SD. Ensuite, GWN génère deux paires de clés secrètes/publiques (x, X) où x ∈ Z*n et X=xP.

A. Phase d'enregistrement du capteur

La passerelle choisit une clé partagée avec le capteur et calcule Xj= h(SIDj||XGWS-SD) avant d'envoyer Xj au capteur. Enfin, Sj calcule Fj=h(SIDj||XGWS-SD) =? Xj ou non. Avant que les capteurs ne stockent SIDj, Fj dans leur mémoire.

B. Phase d'enregistrement de l'utilisateur

- Étape 1 : Ui sélectionne librement une identité IDu et un mot de passe PWu et extrait les informations biométriques sur un appareil mobile avec l'Fuzzy Extractor
- Gen (BIOu) = (Ru, Pu). Ensuite, Ui génère un nombre aléatoire ru et calcule APu=h(PWu||ru||Ru), AIu=h(IDu||ru). Après, Ui soumet une demande (AIu, APu) à GWN de manière sécurisée.
- Étape 2 : Lorsque GWN reçoit des demandes de Ui, il calcule FI=h(AIu||XGWS), XI=h(APu||XGWS-U), et sélectionne un nombre aléatoire K1 et calcule

$$Yi=h\ (K1||XGWS\text{-}U),$$
$$EI=FI\oplus XI,$$
$$Zi=Yi\oplus XI\oplus FI.$$

Enfin, GWN envoie les données (EI, Zi) à Ui de manière sécurisée.

- Étape 3 : Après avoir reçu EI de GWN, Ui calcule

$$XI=h(APu||XGWS\text{-}U),$$
$$FI=EI\oplus XI,$$

Puis stocke (FI, EI, Zi, ru, Pu, Gen(•), Rep(•)) dans sa carte à puce.

C. Phase de connexion et d'authentification

- **Étape 1 :** L'utilisateur Ui entre son identifiant IDu et son mot de passe PWu, et enregistre les données biométriques BIOu sur son appareil mobile. La carte à puce calcule Ru = Rep (BIOu, Pu) à l'aide d'un Fuzzy Extractor.

Ui calcule

$$AIu'=h\ (IDu'||ru),$$
$$APu'=h\ (PWu'||ru||\ Ru),$$
$$XI'=h\ (APu'||XGWS\text{-}U),$$

Ui vérifie si AIu' et XI' sont égaux à AIu et XI respectivement. Si tel est le cas, l'utilisateur a entré les informations d'identité et de mot de passe correctes ainsi que les données biométriques BIOu.

Ensuite, la carte à puce génère un nombre aléatoire a∈Zn*, et calcule :

$$Yi=Zi\oplus XI\oplus FI,$$
$$L1=aP,\ L2=aX,$$
$$DIDU=IDU\oplus L2,$$
$$M3=\ SIDj\oplus Yi\oplus L2,$$

Et obtient la valeur de hachage M4=h (L1|| DIDu || SIDj||Yi).

Ui envoie ensuite le message 1 contenant les éléments {DIDu, L1, M4, and M3} au GWN.

- **Étape 2 :** Le GWN reçoit le message1, et calcule
  L2'=xL1, vérifie IDu'=DIDu⊕L2' et utilise Yi' pour calculer SIDj'=M3⊕Yi'⊕L2'. Enfin, il vérifie si M4=? M4'.
  Le GWN calcule :

$$Xj=h(SIDj||XGWS\text{-}SD),$$
$$M5=IDu\oplus Xj,$$
$$M6=h(L1||SIDj||IDu||Xj).$$

  Il envoie ensuite le message 2 contenant les éléments {L1, M5, M6} au capteur.
- **Étape 3 :** Le capteur reçoit le message 2, calcule Fj, puis IDu=M5⊕Fj et vérifie si M6'=h(L1||SIDj||IDu||Fj) est égal à M6. Si tel est le cas, Sj sait que ces informations proviennent de la passerelle et passe à l'étape suivante. Sinon, le protocole se termine à cette étape.
  Le capteur génère un nonce b∈Zn* et calcule :

$$D3=bP,$$
$$D4=bX,$$

  et calcule la clé partagée SKij entre Ui et Sj :

$$SKij=h\,(IDu||SIDj||b*L1),$$
$$M7=h\,(Fj||D3||SIDj),$$
$$M8=h\,(L1||SKij\,||\,D3),$$

  Il envoie ensuite le message 3 contenant les éléments {D3, M7, M8} à la GWN.
- **Étape 4 :** GWN reçoit le message 3, calcule M7'=h (Xj||D3||SIDj') pour vérifier s'il est égal à M7 ou non, et choisit K2 aléatoirement et calcule :

$$Yinew=h\,(K2||XGWS\text{-}U),$$
$$M9=DIDu'\oplus Yinew\oplus Yi,$$
$$M10=h(DIDu'||L1||D3||Yinew),$$

  GWN envoie ensuite à l'utilisateur le message 4{D3, M8, M9, M10}.
- **Étape 5 :** L'utilisateur Ui reçoit le message 4 de GWN et calcule :

$$Yinew=M9\oplus DIDu\oplus Yi,$$

  Puis vérifie si :

$$M10'=h(DIDu||L1||D3||Yinew)=?\ \text{Égal ou non à M10},$$

  et calcule : $SKij'=h(IDu||SIDj||aD3)=h(IDu||SIDj||ab*P),$
  Après avoir vérifié si :

$$M8'=h(L1||SKij'||D3)=?\ \text{est égal ou non à M8}.$$

  Finalement, l'utilisateur partage une clé de session skij avec le capteur. La phase d'authentification et d'établissement de clé est présentée dans L'algorithme1 et La Figure 4.2.

Ui	GWN	Sj
Ui entre son identifiant IDu et son mot de passe PWu, a carte à puce calcule Ru = Rep (BIOu, Pu). Ui calcule AIu'=h (IDu'‖ru), APu'=h (PWu'‖ru‖ Ru), XI'=h (APu'‖XGWS-U), Ui vérifie si AIu' et XI' sont égaux à AIu et XI Ensuite, la carte à puce génère un nombre aléatoire a∈Zn*, et calcule : Yi=Zi⊕XI⊕FI, L1=aP, L2=aX, DIDU =IDU⊕L2, M3= SIDj⊕Yi⊕L2, M4=h (L1‖ DIDu ‖ SIDj‖Yi). **Mes1= {DIDu, L1, M4, and M3**} → **Mes4= {D3, M8, M9, M10}** ← calcule : Yinew=M9⊕DIDu⊕Yi, Puis vérifie si : M10'=h(DIDu‖L1‖D3‖Yinew)=? Égal ou non à M10, et calcule : SKij'=h(IDu‖SIDj‖aD3)=h(IDu‖SIDj‖ab*P), Après avoir vérifié si : M8'=h(L1‖SKij'‖D3)=? est égal ou non à M8. Finalement, l'utilisateur partage une clé de session skij avec le capteur	calcule L2'=xL1, vérifie IDu'=DIDu⊕L2' et utilise Yi' pour calculer SIDj'=M3⊕Yi'⊕L2'. Enfin, il vérifie si M4=? M4'. Le GWN calcule : Xj=h(SIDj‖XGWS-SD), M5=IDu⊕Xj, M6=h(L1‖SIDj‖IDu‖Xj). **Mes2= {L1, M5, M6}** → **Mes3= {D3, M7, M8}** ← calcule M7'=h (Xj‖D3‖SIDj') pour vérifier s'il est égal à M7 ou non, et choisit K2 aléatoirement et calcule : Yinew =h (K2‖XGWS-U), M9=DIDu'⊕Yinew⊕Yi, M10=h(DIDu'‖L1‖D3‖Yinew).	calcule Fj, puis IDu=M5⊕Fj et vérifie si M6'=h(L1‖SIDj‖IDu‖Fj) est égal à M6. Le capteur génère un nonce b∈Zn* et calcule : D3=bP, D4=bX, et calcule la clé partagée SKij entre Ui et Sj : SKij=h (IDu‖SIDj‖b*L1), M7=h (Fj‖D3‖SIDj), M8=h (L1‖SKij ‖ D3).

Fig 4.2. Phase login et d'authentification.

Algorithme1: Phase login et d'authentification

```
# Étape 1
IDu = input ("Entrez ID : ")
PWu = input ("Entrez PW : ")
BIOu = input ("Entrez BIO : ")
#
# Calcul du Ru avec un Fuzzy Extractor
Ru = Fuzzy Extractor (BIOu, Pu)
# Calcul des valeurs AIu' et APu'
AIu' = hash (IDu || Ru)
APu' = hash (PWu || Ru || Ru)
# Vérification des valeurs AIu' et APu'
if AIu' == AIu and APu' == APu:
    # L'utilisateur a entré les informations correctes
    # Génération du nombre aléatoire a
    a = generate_random_number ()
    # Calcul des valeurs Yi, L1, L2, DIDu, M3
    Yi = Zi ⊕ XI ⊕ FI
    L1 = a * P
    L2 = a * X
    DIDu = IDu ⊕ L2
    M3 = SIDj ⊕ Yi ⊕ L2
    # Calcul de M4
    M4 = hash (L1 || DIDu || SIDj || Yi)
    # Envoi du message 1 au GWN
    Envoyer_un_message_au_GWN ({"DIDu": DIDu, "L1": L1, "M4": M4, "M3": M3})
#
# Étape 2
message1 = message_reçu_par_Ui ()
# Extraction des éléments de message1
```

```
30. DIDu = message1 ["DIDu"]
31. L1 = message1 ["L1"]
32. M4 = message1 ["M4"]
33. M3 = message1 ["M3"]
34. # Calcul de L2'
35. L2’ = x * L1
36. # Vérification de IDu'
37. IDu’ = DIDu ⊕ L2’
38. # Calcul de SIDj’
39. SIDj’ = M3 ⊕ Yi ⊕ L2’
40. # Calcul de Xj, M5, M6
41. Xj = hash (SIDj’ || XGWS_SD)
42. M5 = IDu ⊕ Xj
43. M6 = hash (L1 || SIDj’ || IDu || Xj)
44. # Envoi du message 2 au capteur
45. envoyer_un_message_au_capteur ({"L1": L1, "M5": M5, "M6": M6})
46. #
47. # Étape 3
48. message2 = message_reçu_par_GWN ()
49. # Extraction des éléments de message2
50. L1 = message2 ["L1"]
51. M5 = message2 ["M5"]
52. M6 = message2 ["M6"]
53. # Calcul de Fj
54. Fj = calculate_Fj ()
55. # Vérification de M6’
56. M6’ = hash (L1 || SIDj’ || IDu || Fj)
57. if M6’ != M6:
58.     exit ("Protocole terminé. Étape 3 a échoué.")
59. # Génération du nonce b
60. b = generate_random_nonce ()
61. # Calcul des valeurs D3, D4, SKij
62. D3 = b * P
63. D4 = b * X
64. SKij = hash (IDu ⊕SIDj’ ⊕ b * L1)
65. # Calcul de M7, M8
66. M7 = hash (Fj || D3 || SIDj’)
67. M8 = hash (L1 || SKij || D3)
68. # Envoi du message 3 à GWN
69. envoyer_un_message_au_GWN ({"D3": D3, "M7": M7, "M8": M8})
70. #
71. # Étape 4
72. message3 = message_reçu_par_capteur ()
```

```
# Extraction des éléments de message3
D3 = message3 ["D3"]
M7 = message3 ["M7"]
M8 = message3 ["M8"]
# Calcul de M7'
M7’ = hash (Xj || D3 || SIDj’)
if M7’ != M7:
    exit("Protocole terminé. Étape 4 a échoué.")
# Choix aléatoire de K2
K2 = generate_random_key ()
# Calcul de Yinew, M9, M10
Yinew = hash (K2 || XGWS_U)
M9 = DIDu’ ⊕ Yinew ⊕ Yi
M10 = hash (DIDu’ || L1 || D3 || Yinew)
# Envoi du message 4 à l'utilisateur
envoyer_un_message_au_Ui ({"D3": D3, "M8": M8, "M9": M9, "M10": M10})
#
# Étape 5
message4 = message_reçu_par_GWN ()
# Extraction des éléments de message4
D3 = message4 ["D3"]
M8 = message4 ["M8"]
M9 = message4 ["M9"]
M10 = message4 ["M10"]
# Calcul de Yinew
Yinew = M9 ⊕ DIDu ⊕ Yi
# Vérification de M10'
    M10_’ = hash (DIDu || L1 || D3 || Yinew)
    if M10_’ != M10:
        exit ("Protocole terminé. Étape 5 a échoué.")
    # Calcul de SKij'
    SKij’ = hash (IDu || SIDj’ || a * D3)
    # Calcul de M8'
    M8_’ = hash (L1 || SKij’ || D3)
    if M8’ != M8:
        exit (" Protocole terminé. Étape 5 a échoué.")
    # Partage de la clé de session skij avec le capteur
    skij = generate_session_key ()
    # Fin du protocole avec la clé de session skij partagée
```

4.4 ANALYSE DE SÉCURITÉ

Dans cette section, nous analysons la sécurité de notre schéma et prouvons que notre schéma proposé est sécurisé contre diverses attaques telles que l'attaque interne, l'anonymat de l'utilisateur de la carte intelligente volée/Sensor anonymat...

- **Anonymat de l'utilisateur/Impossibilité de retracer (User anonymity/ Untraceability)**
  Dans notre schéma, l'identité réelle de l'utilisateur Ui n'est pas contenue dans l'un des messages de communication. Dans la demande de connexion M1 = {DIDu, L1, M4 et M3}, l'identité réelle est remplacée par DIDu. De plus, pour obtenir l'identité de Ui à partir de DIDu, la connaissance du nombre aléatoire a est nécessaire, et a est une clé secrète connue uniquement de Ui. Tout adversaire ne peut pas obtenir l'identité à partir de DIDu = IDU⊕L2, où L2 = aX. Ainsi, notre schéma assure l'anonymat de l'utilisateur. Notre schéma assure l'impossibilité de retracer, qui est obtenue grâce au nombre aléatoire a et à la valeur Yi générée par l'utilisateur.

- **Anonymat du capteur (Sensor anonymity)**
  Dans notre schéma, le dispositif du capteur Sj assure l'anonymat du capteur. Dans n'importe quel message de communication, l'adversaire A ne peut pas obtenir l'identité réelle à partir de M3 = SIDj⊕Yi⊕L2 sans connaître Yi et a. Par conséquent, notre schéma assure l'anonymat du capteur.

- **Attaque par carte intelligente volée (Stolen smart card attack)**
  Dans le schéma proposé, la carte intelligente de l'utilisateur contient les paramètres secrets (FI, EI, Zi et ru, Pu, Gen (•), Rep (•)), où

$$FI=h(AIu||XGWS),$$
$$EI=FI⊕XI= h(APu||XGWS\text{-}U),$$
$$Zi= FI⊕XI⊕Yi =h(K1||XGWS\text{-}U).$$

  L'adversaire A qui vole la carte intelligente et obtient les paramètres (FI, EI, Zi et ru, Pu, Gen (•), Rep (•)) ne peut pas obtenir l'identité et le mot de passe réels de Ui sans connaître la clé secrète XGWN de GWN et le nombre aléatoire K1 et la clé partagée XGWN-SD. Par conséquent, A ne peut pas se faire passer pour l'utilisateur. De plus, notre protocole est résistant à l'attaque par carte intelligente volée.

- **Attaque interne (Insider attack)**
  Lorsque Ui envoie le message de demande d'inscription (AIu, APu) à GWN, au lieu de PWu, il est nécessaire pour A d'obtenir le nombre aléatoire ru et la clé secrète Ru à partir de APu afin d'obtenir PWu. L'adversaire ne peut pas obtenir le mot de passe PWi de Ui à partir de APu sans connaître le nombre aléatoire ru et la clé secrète Ru. Par conséquent notre schéma est résistant à l'attaque interne.

- **Confidentialité avancée (Forward secrecy)**

  L'établissement de la clé de session SKij=h (IDu||SIDj||b*L1) inclut :

  IDu,
  L1=aP,
  SIDj,
  D3=bP.

  Donc la confidentialité avancée signifie que l'attaquant A ne peut pas affecter la confidentialité des communications passées sans connaître L1 et D3. De plus, notre schéma offre une confidentialité avancée.

- **Authentification mutuelle**

  Dans notre protocole, l'utilisateur Ui et le dispositif de capteur s'authentifient mutuellement en vérifiant M8'=M8, afin que Ui et la passerelle s'authentifient mutuellement en vérifiant respectivement M4 et M10, GWN et Sj en vérifiant respectivement M6 et M7. Le schéma proposé offre une authentification mutuelle.

- **Clé de session**

  Dans notre schéma, la clé de session établie peut être utilisée pour sécuriser la communication entre Ui et Sj, la clé de session calculée dans notre schéma étant :

  SKij=h (IDu||SIDj||aD3) =h (IDu||SIDj||ab*P).

  De sorte qu'aucune tierce partie ne peut connaître Skij. Par conséquent, le schéma proposé fournit avec succès une clé de session.

4.5 **CONCLUSION**

En conclusion, notre analyse du protocole de Yuwen et al. a révélé des vulnérabilités persistantes face à diverses attaques, telles que les attaques internes ou par vol de carte intelligente, compromettant ainsi la robustesse du système dans les environnements IdO.

Pour remédier à ces lacunes, nous avons proposé un protocole d'authentification mutuelle et d'établissement de clé sécurisé, utilisant un Fuzzy Extractor et le cryptage ECC pour garantir l'anonymat, l'impossibilité de traçage et la confidentialité des données échangées. Cette solution offre aux utilisateurs et aux capteurs une protection robuste contre les attaques potentielles, réduisant considérablement les risques associés aux attaques internes ou par vol de carte intelligente. En garantissant la sécurité et la confidentialité des informations, ce protocole représente une avancée significative dans la sécurisation des environnements IdO.

CHAPITRE 5: AUTHENTIFICATION SECURISEE AVEC ECC POUR LA PROTECTION DE LA VIE PRIVEE DANS LES CONCEPTS IDO

5.1 **INTRODUCTION**

Depuis la fin des années 1980, Internet a connu une évolution majeure, l'IdO représente une infrastructure mondiale pour la société de l'information, permettant l'interconnexion d'objets physiques ou virtuels avec des technologies de l'information et de la communication. Cette révolution numérique, estimée par l'Institut Gartner à plus de 50 milliards d'objets connectés, impacte divers domaines tels que l'industrie, l'agriculture, la sécurité, la maison intelligente, le transport et la santé.

L'objectif de l'IdO est de coordonner les interactions entre des éléments agissant à la fois comme capteurs et actionneurs, communément appelés objets. Ces objets introduisent de nouvelles applications dans nos vies, permettant un contrôle à distance des appareils intelligents via des canaux ouverts. Cependant, cette connectivité omniprésente soulève des préoccupations quant à la sécurité et à la confidentialité des données, car chaque appareil IdO devient un collecteur de données potentiel.

Ainsi, avant toute mise en œuvre de l'IdO, il est impératif de prendre en compte les risques potentiels en matière de sécurité et de confidentialité.

Cette étude se concentre sur ces aspects en proposant un nouveau système d'authentification pour l'Internet des objets. Ce protocole, basé sur ECC et un Fuzzy Extractor, vise à assurer la sécurité des données des capteurs IdO lors de leur transmission et de leur stockage en utilisant des techniques de cryptage et d'authentification robustes. Les principales contributions de ce travail comprennent la sécurité contre diverses attaques, une vérification formelle de la solidité du protocole, une analyse de l'authentification mutuelle et de l'établissement de clés de session, ainsi qu'une comparaison avec d'autres travaux similaires en termes de coûts de calcul et de communication.

5.1.1 **Hypothèses et Modèle du réseau**

La performance d'un protocole de sécurité est influencée par plusieurs facteurs, notamment le mécanisme de sécurité utilisé, l'architecture du réseau et le scénario de communication. Afin d'évaluer la sécurité d'un protocole, il est essentiel de prendre en compte les caractéristiques propres au réseau sur lequel il sera déployé. Dans notre cas spécifique, une mise en œuvre typique de l'IdO implique trois types de nœuds : les nœuds utilisateur (Ui), les nœuds passerelle (GWN) et les dispositifs IdO (Sj). Les dispositifs IdO sont connectés à l'Internet public via leurs nœuds passerelle respectifs, le dispositif IdO détecte et collecte des informations et envoie des données à la passerelle qui envoie les informations au nœud utilisateur. Les nœuds utilisateur responsables doivent s'inscrire auprès de leurs nœuds passerelle respectifs avant d'accéder à leur dispositif intelligent correspondant (Sj). L'utilisateur peut s'authentifier lorsqu'il accède à Sj via GWN pour négocier une clé de réunion (session) afin d'accéder aux données du dispositif IdO, comme décrit dans la Figure 5.1.

- GWN : Il est considéré comme une partie de confiance et est responsable de l'inscription de chaque utilisateur et capteur.
- Ui : l'utilisateur qui possède un dispositif intelligent obtient son pseudo-identité auprès de GWN lors de la phase d'inscription.
- Sj : Les capteurs obtiennent également leurs clés secrètes auprès de GWN lors de la phase d'inscription.

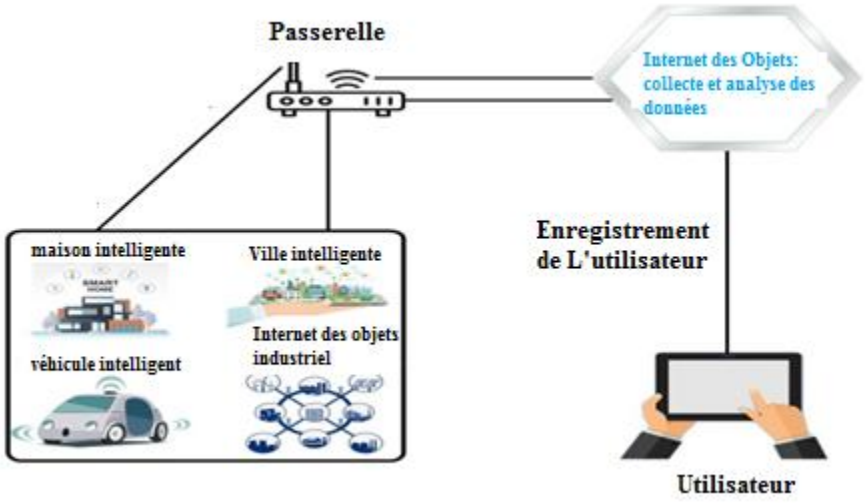

Fig 5.1. La structure du modèle du réseau.

5.2 **PRÉLIMINAIRES MATHÉMATIQUES**

Dans cette section, commence par la présentation des notations et se poursuit avec une brève introduction de Fuzzy Extractor pour la vérification biométrique et de la cryptographie à courbes elliptiques(ECC).

5.2.1 **Notations**

Le Tableau 5.1 assume un rôle de grande importance au sein du protocole proposé, étant donné qu'il se charge d'énumérer de manière exhaustive toutes les notations utilisées, en fournissant une référence essentielle pour la compréhension et l'interprétation des différentes variables, symboles et abréviations qui sont employés tout au long du protocole.

Notations	Description
U_i, GWN	L'utilisateur et la passerelle.
Sj	Le dispositif IdO
SC	La carte à puce
IDi	L'identité de l'utilisateur
SIDj	L'identité du capteur
PWi	Le mot de passe de l'utilisateur
PIDi	Pseudo-identité assignée par GWN
BIOi	La biométrie de l'utilisateur Ui
a, e, b, c	Nombres aléatoires
SKi	La clé de session
Xs	La clé secrète de GWN
G	Le générateur de la courbe elliptique
ɛ̇	Adversaire L'attaquant
h	La fonction de hachage
||	Connecte deux chaînes de caractères ensemble
⊕	Opération XOR

Tab 5.1. Tableau des notations

5.2.2 **Fuzzy Extractor**

Fuzzy Extractor a été introduit par [84] pour traiter les informations biométriques. Il existe deux mécanismes pour vérifier les informations biométriques : le bio-hash et l'extracteur flou. Fuzzy Extractor repose sur des algorithmes sécurisés qui peuvent être utilisés pour générer des clés de chiffrement à partir de données biométriques bruyantes. Le processus d'identification de l'utilisateur peut être utilisé pour récupérer les informations biométriques. Fuzzy Extractor se compose d'une méthode de génération probabiliste Gen (•) et d'une méthode de reproduction déterministe Rep (•).

1) Gen (•) : Sur le modèle biométrique de l'utilisateur Ui, appelé BIOi, Gen (•) renvoie une paire ayant un biométrique, la chaîne de clé secrète σi de bits, $\sigma i \in \{0,1\}^a$ pour l'utilisateur U, et son paramètre public d'aide correspondant (reproduction) τi, c'est-à-dire que Gen (BIOi) = (σi, τi).
2) Rep (•) : Étant donné un modèle biométrique bruyant BIOi de l'utilisateur Ui, Rep (•) signifie que la clé secrète σi peut être récupérée par le modèle biométrique d'origine et avec le paramètre d'aide τi, avec le critère que la distance de Hamming entre le modèle biométrique d'origine BIOi et le modèle biométrique courant BIO'i ne dépasse pas une valeur de seuil de tolérance d'erreur t. Ainsi, Rep (BIO'i, τi) = σi.

5.2.3 **La cryptographie à courbe elliptique (ECC)**

La cryptographie à courbe elliptique (ECC) a été proposée par [74], [75]. Une courbe elliptique est une méthode basée sur la structure algébrique. Elle permet une sécurité plus importante pour une taille de clé donnée et est très difficile à régénérer par un attaquant car la clé est générée à partir de la ligne sur la courbe, contrairement aux techniques de cryptographie conventionnelles telles que RSA. Une clé ECC de 256 bits offre le même niveau de protection qu'une clé RSA de

3072 bits. L'utilisation de clés plus petites signifie qu'elle consomme moins d'espace de stockage et de bande passante pendant la transmission.

Soit p > 3 un nombre premier, le champ d'ordre q est composé de tous les points (x, y), avec

$$x, y \in Fp \text{ tels que}$$

$$4a3 + 27\ b2 \neq 0 \bmod p,$$

L'équation ci-dessus peut être simplifiée en y2=x3+ax+b mod p [76].

5.3 **LA SOLUTION PROPOSÉE**

Un schéma d'authentification avec anonymat de l'utilisateur et d'établissement de clé pour l'IdO utilisant ECC, la biométrie et Fuzzy Extractor est proposé. Le schéma suggéré se compose de quatre phases : l'inscription, l'authentification, l'établissement de clé et la phase de changement de mot de passe. Ces phases permettent d'atteindre une authentification entre l'utilisateur et les capteurs avec l'aide de GWN.

5.3.1 **Phase d'enregistrement**

Cette phase est divisée en deux parties, à savoir l'enregistrement du capteur et l'enregistrement de l'utilisateur.

- **Phase d'enregistrement du capteur**

  GWN calcule xj = h (SIDj || Xs) et envoie xj au capteur avant de stocker le SIDj et xj dans sa mémoire.

- **Phase d'enregistrement de l'utilisateur**

  Dans notre système, GWN effectue la tâche d'inscription de l'utilisateur. Cette étape est effectuée sur un canal sécurisé comme suit :

  - Ui insère les identifiants IDi, PWi et les empreintes BIOi dans la carte à puce en utilisant Fuzzy Extractor Gen (BIOi) = (RU, PU).
  - SC calcule :

    $$Ai = h (IDi \| PWi \| Ru),$$

    $$Di = h (IDi \| h(Ru) \| PWi).$$

    Ensuite, il soumet {IDi, Ai} à GWN via un canal sécurisé.

  - GWN attribue un PIDi aléatoire en tant que pseudo-identité à Ui et calcule :

    $$Ki = Ai \oplus h(Xs \| PIDi),$$

    $$xi = h(Xs \| IDi).$$

    Ensuite, GWN stocke {Ki, PIDi et xi} dans sa base de données et envoie à Ui {PIDi, xi} via un canal sécurisé.
  - Ui met les paramètres dans SCi {Di, PU, PIDi, xi, Gen(.), Rep(.)}.

- **Phase d'authentification et d'établissement de clé**

  Lorsque l'utilisateur souhaite accéder aux données des appareils IdO, l'interface utilisateur (Ui) et le serveur doivent s'authentifier mutuellement. La phase d'authentification et d'établissement de clé est présentée dans le Tableau 5.2.

  - **Étape 1 :** Ui insère SC dans un lecteur de carte et entre l'identité IDi, PWi et les empreintes BIOi' avec extracteur flou. Le SC calcule :

    $$RU = Rep (BIOi', PU),$$
    $$Di* = h (IDi \| h(Ru) \| PWi)$$

    et vérifie si Di*? = Di. Si ce n'est pas le cas, la demande de connexion sera rejetée par le SC si au moins l'un des facteurs d'identification, de mot de passe et de biométrie est invalide. Sinon, Ui calcule : Ai = h (IDi || PWi || Ru).

    Ensuite, Ui génère un nombre aléatoire a, e ∈ Zn* et calcule :

    $$M1 = a•G,$$
    $$B = Ai \oplus M1,$$
    $$L1 = IDu \oplus h (PIDi \| Ai \| M1),$$
    $$L2 = (SIDj \| e) \oplus Ai,$$
    $$L3 = h (IDi \| D2 \| Ai \| e).$$

    Enfin, la demande de connexion Mes1 = {PIDi, B, L1, L2, L3} est soumise à GWN.

  - **Étape 2 :** GWN, lors de la réception de la demande de connexion, obtient K en utilisant PIDi, après avoir récupéré Ai = Ki ⊕ h(Xs || PIDi).

    GWN calcule :

    $$M1* = Ai \oplus B,$$
    $$IDi = L1 \oplus h (PIDi \| Ai \| M1*)$$

    GWN vérifie si l'IDi de Ui est dans la base de données. Si tel est le cas, récupère SIDj ⊕ e = D2 ⊕ Ai ; et vérifie si L3*? = L3. Après cela, GWN génère un nombre aléatoire b et calcule :

    $$L4 = h (SIDj \| Xs),$$
    $$L5 = (IDi \| GID \| M1 \| |b\|\|e) \oplus L4,$$
    $$L6 = h (IDi \| GID \| M1 \| L4 \| b \| e).$$

    Ensuite, GWN soumet le message Mes = {L5, L6} à Sj.

  - **Étape 3 :** Sj, lorsqu'il reçoit le message de GWN, calcule :

    $$(IDi \| GID \| M1 \| b \| e) = xj \oplus L5,$$
    $$L6* = h (IDi \| GID \| M1 \| L4 \| b \| e),$$

    Sj vérifie si L6*? = L6, sinon ; Sj génère un nombre aléatoire c ∈ Zn*, et calcule :

    $$M2 = c•G,$$
    $$SKi = h (IDi \| SIDj \| GID \| c•M1 \| e \| b),$$
    $$L7 = xj \oplus M2, Auth = h (SIDj \| xj \| M2).$$

    Ensuite, Sj transmet le message Mes3 = {L7, Auth} à GWN.

- **Étape 4:** GWN reçoit Mes3, puis calcule: M2* = L4 ⊕ L7 et vérifie si Auth*? = Auth. La session est terminée si Auth* ≠ Auth. Sinon, GWN sélectionne PIDinew et calcule: Kinew = Ai⊕h (Xs||PIDinew), Stocke {Kinew, PIDinew} dans sa base de données, puis GWN calcule:

$$L8 = (GID||b||M2) \oplus xi,$$
$$L9 = PIDinew \oplus xi,$$
$$Auth2 = h (GID||b||xi||M2||PIDinew).$$

- Ensuite, GWN soumet le message Mes4 = {L8, L9, Auth2} à Ui.

- **Étape 5 :** Lorsqu'Ui reçoit Mes4, il calcule :

$$PIDinew=L9 \oplus xi,$$
$$L8 \oplus xi= (GID||b||M2),$$
$$SKi=h (IDi||SIDj||GID||c•M1||e||b),$$

Après vérification Auth2* =? Auth2. Si la session n'est pas maintenue, elle est terminée. Sinon, Ui remplace PIDi par PIDinew. Enfin, Ui authentifie GWN et partage une clé de session SKi avec Sj.

- **Phase de Changement de Mot de Passe**

Cette phase commence lorsqu'Ui souhaite changer le mot de passe d'un utilisateur. Tout le processus est détaillé ci-dessous :

- Insérer SC dans un lecteur de carte, entrer IDi, PWi et imprimer BIOi* dans la carte intelligente avec un extracteur flou.
- Le SC calcule :

$$RU =Rep (BIOi*, PU),$$
$$Di* = h (IDi||h (Ru) ||PWi).$$

- Vérifie si Di*? = Di. Si cela n'est pas le cas, la demande de connexion sera rejetée par le SC. Sinon, la carte intelligente passera à l'étape suivante.
- Lorsqu'il reçoit le nouveau mot de passe choisi (PWinew) d'Ui, la carte intelligente calcule :

$$Ainew = h (IDi||PWinew||Ru),$$
$$Dinew = h (IDi||h (Ru) ||PWinew).$$

- Ensuite, le SC remplace Ai et Di par (Ainew) et (Dinew), respectivement.

Tab 5.2. La Phase login et d'authentification.

Ui	GWN	Sj
Inputs IDi and PWi Imprints BIOi' and Calculates R_U=Rep (BIOi', P_U) Di* = h (IDi‖h (Ru)‖PWi) Checks Di* ?= Di, computes Ai = h (IDi‖PWi‖Ru) Ui generates a random number a, e∈ Zn* M1=aG B=Ai⊕ M1 L1=IDi⊕ h(PIDi‖Ai‖M1) L2=(SIDj‖ e)⊕ Ai L3=h(IDi‖L2‖Ai‖e)		
Mes1= {PIDi, B, L1, L2, L3} →		
	Obtains Ki using PIDi Retrieves Ai=Ki⊕ h(Xs‖PIDi) Computes M1*=Ai⊕ B IDi*=L1⊕ h(PIDi‖Ai‖M1*) Retrieves(SIDj‖ e*)=L2⊕Ai And verifiesL3*=h(IDi*‖L2‖Ai‖e*) L3*=? L3 Generates a random number b ComputesL4=h(SIDj‖Xs) L5=(IDi‖GID‖M1‖b‖e) ⊕ L4 L6=h(IDi‖GID‖M1‖L4‖b‖e)	
	Mes2= {L5, L6} →	
		Checks(IDi‖GID‖M1‖b‖e) =xj ⊕ L5 L6*=h(IDi‖GID‖M1‖L4‖b‖e) ChecksL6*? =L6 Generates a random number c∈ Zn* M2=cG SKi=h(IDi‖SIDj‖GID‖cM1‖e‖b) L7=xj⊕M2 Auth=h(SIDj‖xj‖M2)
	← Mes3= {L7, Auth}	
	CalculatesM2*=L4 ⊕ L7 Checks Auth*? = Auth Selects PIDinew and computes Kinew=Ai⊕h (Xs‖PIDinew) GWN stores{Kinew, PIDinew}in its DB and CalculatesL8=(GID‖b‖M2) ⊕ xi L9=PIDinew ⊕ xi Auth2=h(GID‖b‖xi‖M2‖PIDinew)	
← Mes4= {L8, L9, Auth2}		
Calculates PIDinew=L9 ⊕ xi L8⊕ xi=(GID‖b‖M2) SKi=h(IDi‖SIDj‖GID‖aM2‖e‖b) Auth2*=h(GID‖b‖xi‖M2‖PIDinew) CheckAuth2* ?= Auth2 Ui replaces PIDi with PIDinew Ui and Sj establish session key SKi and complete the authentication.		

5.4 ANALYSE DE SÉCURITÉ

Dans cette section, les objectifs de sécurité du schéma proposé sont analysés de manière formelle en utilisant l'outil de logique de Burrows-Abadi-Needham (BAN). La sécurité du schéma est évaluée à l'aide d'une analyse informelle et comparée aux travaux antérieurs.

5.4.1 Vérification formelle

Le protocole d'authentification est crucial pour la sécurité des systèmes IdO. Pour assurer une authentification mutuelle sécurisée entre un diverses nœuds IdO, nous avons utilisé la logique Burrows-Abadi-Needham (BAN) [85], [86], une méthode populaire pour décrire et analyser les protocoles d'authentification.

En effet, la logique BAN a été largement utilisé pour la vérification formelle des protocoles de sécurité et pour prouver la justesse de tout protocole d'authentification. Dans cette sous-section, nous fournissons une introduction brève mais essentielle aux symboles et aux règles dans les tableaux 5.3 et 5.4, respectivement. De la logique BAN. Grâce à cette approche, nous pouvons prouver que notre schéma d'authentification est sûr et fiable pour une utilisation dans les systèmes IdO.

P| ≡ X	P believes X.
P◁X	P sees X, i.e. P has received message X and may read it.
♯ (X)	X is fresh.
(X, Y)	X or Y is a part of a message (X, Y).
P |∼ X	P once said X or P has sent message X.
P ⇒ X	P has jurisdiction over X.
⟨X⟩Y	X is encrypted with Y.
(X)K	X is hashed with the K.
$P \overset{k}{\leftrightarrow} Q$	P and Q can communicate with the shared key K.

Tab 5.3. Les notations utilisées dans BAN logic [87].

R1. Message meaning rule	$\frac{P\| \equiv P \overset{k}{\leftrightarrow} Q,\ P \lhd \langle X\rangle y}{P\ \| \equiv Q\ \| \sim X}$
R2. Nonce verification rule	$\frac{P\| \equiv \sharp(X), P\| \equiv Q\| \sim X}{P\ \| \equiv Q\ \| \equiv X}$
R3. Jurisdiction rule	$\frac{P\| \equiv Q \Rightarrow X, P\ \| \equiv Q\ \| \equiv X}{P\ \| \equiv X}$

R4. Freshness rule	$\frac{P\mid \equiv \sharp(X)}{P\mid \equiv \sharp(X,Y)}$
R5. Belief rule	$\frac{P\mid \equiv (X), P\mid \equiv (Y)}{P\mid \equiv (X,Y)}$
R6. Session keys rule	$\frac{P\mid \equiv \sharp(X), P\mid \equiv Q\mid \equiv X}{P \overset{k}{\leftrightarrow} Q}$

Tab 5.4. Les règles utilisées dans BAN logic [87].

Les hypothèses suivantes sont présentées dans la table 5.5.

- Dans le schéma proposé, les messages envoyés via le canal ouvert sont les suivants :

Message 1: Ui → GWN {PIDi, B, L1, L2, L3}

Message 2: GWN → Sj {L5, L6}

Message 3: Sj → GWN {L7, Auth}

Message 4: GWN → Ui {L8, L9, Auth2}

- Les objectifs :

$$Obj1: Ui \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$$

$$Obj2: Ui \mid\equiv Sj \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$$

$$Obj3: Sj \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$$

$$Obj4: Sj\mid\equiv Ui\mid\equiv (Ui \overset{SKi}{\leftrightarrow} S)$$

Hypothése1:	$Ui\mid\equiv \#(a, e)$
Hypothèse 2:	$GWN\mid\equiv \#(b, e)$
Hypothèse 3:	$Sj\mid\equiv \#(c)$
Hypothèse 4:	$Ui\mid \equiv Ui \overset{h(PID\,\|\|Ai\,\|\|M1)}{\longleftrightarrow} GWN$
Hypothèse 5:	$GWN\mid \equiv GWN \overset{h(PID\,\|\|Ai\,\|\|M1)}{\longleftrightarrow} Ui$
Hypothèse 6:	$GWN\mid \equiv GWN \overset{h(SIDj\,\|\|Xs))}{\longleftrightarrow} Sj$
Hypothèse 7:	$Sj\mid \equiv Sj \overset{h(SIDj\,\|\|Xs)}{\longleftrightarrow} GWN$
Hypothèse 8:	$Ui\mid\equiv Sj \mid\Rightarrow c, SIDj, SKi, ca\cdot G$
Hypothèse 9:	$Ui \mid\equiv GWN \mid\Rightarrow b, GID$
Hypothèse 10:	$Sj \mid\equiv Ui \mid\Rightarrow a, e, Ui, SKi, ca\cdot G$
Hypothèse 11:	$Sj \mid\equiv GWN \mid\Rightarrow b, GID$

Tab 5.5. Les hypothèses [87].

Ensuite, en utilisant les règles logiques et les hypothèses BAN, l'authentification mutuelle entre Ui et Sj est démontrée comme suit :

L1. Selon le message1, nous obtenons

GWN◃ {<IDi>h(PIDi||Ai||M1), <a•G> h (IDi||PWi||Ru), <e||SIDj>h (IDi|(|PWi|)|Ru), (IDi||e) h (IDi|(|PWi|)|Ru)}

L2. En utilisant L1, Hypothése5 et la règle de signification des messages, nous obtenons GWN |≡ Ui |~ {<IDi>h(PIDi||Ai||M1), <a•G> h (IDi||PWi||Ru), <e||SIDj>h (IDi|(|PWi|)|Ru), (IDi||e) h (IDi|(|PWi|)|Ru)}

L3. En utilisant Hypothése2 et la règle de concaténation de fraîcheur, nous obtenons GWN|≡# {<IDi>h(PIDi||Ai||M1),<a•G> h (IDi||PWi||Ru), <e||SIDj>h (IDi|(|PWi|)|Ru), (IDi||e) h (IDi|(|PWi|)|Ru)}

L4. En utilisant L2, L3 et la règle de vérification de nonce, nous obtenons GWN |≡ Ui |≡ {<IDi>h(PIDi||Ai||M1), <a•G> h (IDi||PWi||Ru), <e||SIDj>h (IDi|(|PWi|)|Ru), (IDi||e) h (IDi|(|PWi|)|Ru)}

L5. Selon le message2, nous obtenons Sj ◃ {< IDi, GID, M1, b, e >h (SIDj||Xs), (IDi, GID, M1, b, e) h (SIDj||Xs)}

L6. En utilisant Hypothése7, L5 et la règle de signification des messages, nous obtenons Sj |≡ GWN |~ {< IDi, GID, M1, b, e >h (SIDj||Xs), (IDi, GID, M1, b, e) h (SIDj||Xs)}

L7. À partir de Hypothése3 et de la règle de concaténation de fraîcheur, nous obtenons Sj |≡# {< IDi, GID, M1, b, e >h (SIDj||Xs), (IDi, GID, M1, b, e) h (SIDj||Xs)}

L8. À partir de L7, L6 et de la règle de vérification de nonce, nous obtenons Sj |≡ GWN |≡ {< IDi, GID, M1, b, e >h (SIDj||Xs), (IDi, GID, M1, b, e) h (SIDj||Xs)}

L9. Selon le message3, nous obtenons GWN ◃ {< c•G >h (SIDj||Xs), (SIDj, c•G) h (SIDj||Xs)}

L10. En utilisant Hypothése6, L9 et la règle de signification du message, nous obtenons GWN |≡ Sj |~ {< c•G >h (SIDj||Xs), (SIDj, c•G) h (SIDj||Xs)}

L11. À partir de Hypothése2 et de la règle de fraîcheur-concaténation, nous obtenons Sj |≡# {< c•G >h (SIDj||Xs), (SIDj, c•G) h (SIDj||Xs)}

L12. À partir de L10, L11 et de la règle de vérification de nonce, nous obtenons GWN |≡ Sj |≡ {< c•G >h (SIDj||Xs), (SIDj, c•G) h (SIDj||Xs)}

L13. Selon le message4, nous obtenons Ui ◃ {<GID, b, c•G >h (IDi||Xs), <PIDinew>h (IDi||Xs), (GID, b, c•G, PIDinew) h (IDi||Xs)} L14. En utilisant Hypothése4,

L13 et la règle de signification du message, nous obtenons Ui |≡ GWN |~ {<GID, b, c•G >h (IDi||Xs), <PIDinew>h (IDi||Xs), (GID, b, c•G, PIDinew) h (IDi||Xs)}

L15. À partir de Hypothése1 et de la règle de fraîcheur-concaténation, nous obtenons Ui |≡# {<GID, b, c•G >h (IDi||Xs), <PIDinew>h (IDi||Xs), (GID, b, c•G, PIDinew) h (IDi||Xs)}

L16. À partir de L14, L15 et de la règle de vérification de nonce, nous obtenons Ui |≡ GWN |≡ {<GID, b, c•G >h (IDi||Xs), <PIDinew>h (IDi||Xs), (GID, b, c•G, PIDinew) h (IDi||Xs)}

L.18 From L12, L16 and SKi=h (IDi||SIDj||GID||cM1||e||b) we have

$Ui \mid\equiv Sj \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$ (Obj**2**)

L.19 From L4, L8 and SKi=h (IDi||SIDj||GID||cM1||e||b) we have $Sj \mid\equiv Ui \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$ (Obj**4**)

L.20 From L18, A8, Hypothése9 and jurisdiction rule, we have

$Ui \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$ (Obj**1**)

L.21 From L19, Hypothése10, Hypothése11 and jurisdiction rule, we have $Sj \mid\equiv (Ui \overset{SKi}{\leftrightarrow} Sj)$ (Obj**3**)

Moreover, with the steps of BAN Logic, the proposed scheme can successfully achieve mutual authentication and establishment session key between user and IdO device with the help of Gateway (GWN).

5.4.2 **Vérification formelle de sécurité (AVISPA)**

Cette section utilise l'outil d'analyse automatisée puissant de validation des protocoles de sécurité Internet et des applications (AVISPA) [88]. La sécurité informatique est un domaine en constante évolution et la protection des systèmes informatiques est devenue un enjeu majeur pour les entreprises, les gouvernements et les particuliers. Les protocoles de sécurité sont un élément clé de cette protection, car ils sont utilisés pour sécuriser les échanges de données entre les différents éléments du système. Cependant, ces protocoles peuvent présenter des vulnérabilités et des failles de sécurité qui peuvent être exploitées par des attaquants malveillants.
Pour garantir la sécurité des protocoles de sécurité, il est nécessaire de les analyser en détail pour détecter les faiblesses et les brèches potentielles. Pour ce faire, des outils d'analyse de protocoles ont été développés, tels que AVISPA (Automated Validation of Internet Security Protocols and Applications) [88].

AVISPA est un simulateur conçu pour effectuer des tests et des examens sur les protocoles de sécurité informatique. Il utilise différentes techniques analytiques pour garantir la sécurité des protocoles contre les attaques telles que les attaques par rejeu et les attaques de type man-in-the-middle. AVISPA utilise le "High-Level Protocol Specification Language (HLPSL)" pour écrire les protocoles à analyser. Le traducteur HLPSL2IF convertit ensuite le protocole en "Intermediate Format (IF)" [88], qui est introduit dans les back-ends de l'outil AVISPA (voir la figure 5.2).

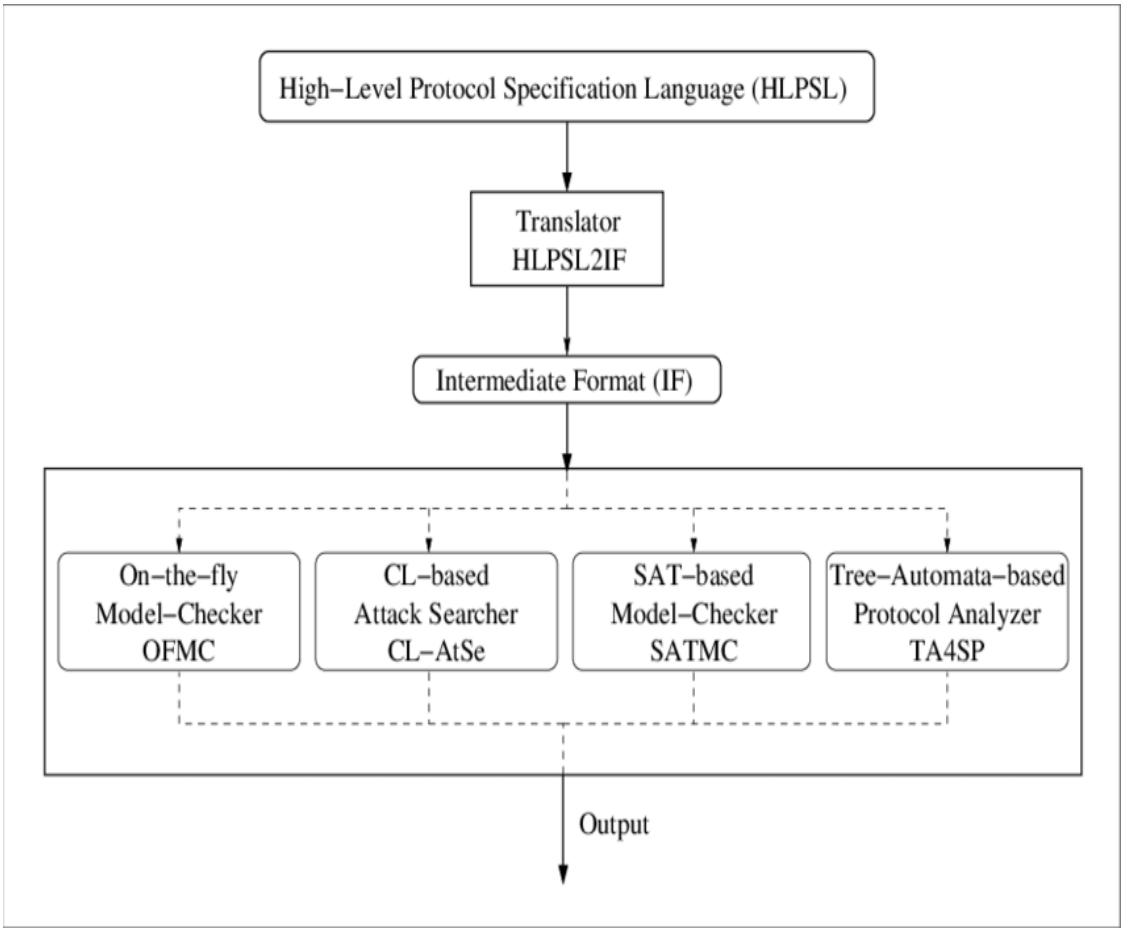

Fig 5.2. L'architecture de l'outil AVISPA [89].

AVISPA utilise différentes techniques analytiques pour vérifier la sécurité des protocoles, notamment :

- Le Contrôleur de modèle à la volée (OFMC),
- La Recherche d'attaque basée sur la logique des contraintes (CL-AtSe),
- Le Vérificateur de modèle basé sur SAT (SATMC),
- Les Automates arborescents basés sur des approximations automatiques pour l'analyse des protocoles de sécurité (TA4SP).

Le format de sortie (OF) fournit une description détaillée de la sûreté du protocole testé. En conclusion, l'analyse de la sécurité des protocoles est une étape cruciale pour garantir la protection des systèmes informatiques. Des outils tels que AVISPA permettent de détecter les faiblesses et les brèches potentielles dans les protocoles de sécurité, contribuant ainsi à renforcer la sécurité informatique.

La sécurité du schéma proposé contre des attaques telles que les attaques de rejeu et de l'homme du milieu est formellement analysée et garantie à l'aide de l'outil AVISPA.

Cette simulation est exécutée dans une machine virtuelle SPAN avec 2048 Mo de RAM, le système d'exploitation Ubuntu10.10-light. L'implémentation HLPSL du schéma proposé

comprend trois rôles de base : un utilisateur, la passerelle et un dispositif intelligent. Deux rôles obligatoires pour la session, l'objectif et l'environnement sont également définis dans le HLPSL. Les spécifications de user, sensor, gateway, sont présentées dans les figures 5.3 et 5.4, 5.5, respectivement. Il convient également de noter que AVISPA met en œuvre le modèle de menace Dolev-Yao (DY) [90]. Ensuite, le schéma proposé est évalué contre les attaques de rejeu et de l'homme du milieu lors du module complémentaire On-the-fly Model checker (OFMC) à l'aide de SPAN.

De plus, les résultats de simulation présentés dans la figure 5.6 montrent que les fonctionnalités de sécurité du schéma proposé sont protégées contre des attaques bien connues.

```
Role user (Ui: agent, Sj: agent, GW: agent,
 Xi: symmetric_key,
 H: hash_func,
 P: text,
 SND_UG, RCV_UG: channel (dy))
 Played_by Ui
 Def=
 Local State: nat,
 PWi, Bioi, IDi, Ai, M1, S0, B: text, D1, Ru, D2, D3, GID, SK,
 Bb, Xs: text,
 M2, PIDinew, SIDj, Aa, Ee, PIDi: text
 Const aa, bb, cc, zz, ii, sc_user_id, sc_sensor_id, user_sensor_sc,
 sensor_user_sc: protocol_id
 init State: = 0
 Transition
  1. State = 0 /\ RCV_UG (start) =|>
  State':= 1    /\ secret ({Xs}, aa, {GW})
                /\ secret ({PIDi}, ii, {Ui, GW})
                /\ secret ({Ru}, cc, {Ui})
                /\ secret ({IDi}, sc_user_id, {Ui})
                /\ secret ({PWi, Bioi}, bb, {Ui})
                /\ secret ({SIDj}, sc_sensor_id, {Sj, GW})
                /\ Ai':= H (IDi.PWi.Ru)
                /\ SND_UG ({Ai'.IDi} _Xi)
  2. State =1 /\ RCV_UG ({PIDi.S0'} _Xi) =|>
     State':=2 /\ Aa':= new ()
                /\ Ee':= new ()
                /\ M1':= exp (Aa'.P)
                /\ B':= xor (Ai, M1')
                /\ D1':= xor (IDi, H (PIDi.Ai.M1'))
                /\ D2':= xor ((SIDj.Ee'), Ai)
                /\ D3':= H (IDi.D2'.Ai.Ee')
                /\ SND_UG (PIDi.B'.D1'.D2'.D3')
  3. State =2  /\ RCV_UG(xor((GID'. Bb'. M2'), S0').  xor (PIDinew', S0').
     H (GID'. Bb'. S0'. M2'. PIDinew')) =|>
     State':= 3 /\PIDi':= PIDinew'
                 /\SK':=H (IDi.SIDj.GID'.exp (Aa.M2').Ee.Bb')
                 /\witness (Ui, Sj, user_sensor_sc, SK')
                 /\request (Ui, Sj, sensor_user_sc, SK')
                 /\request (Ui, GW, zz, S0')
 End role
```

Fig 5.3. Code HLPSL pour le rôle de User

```
Role sensor (Sj: agent, Ui: agent, GW: agent,
H: hash_func,
P: text,
SND_SG, RCV_SG: channel (dy))
Played_by Ui
Def=
local State: nat,     IDi, Bioi, PWi, M1, D4, D5, D7, S1, Xs: text,
PIDi, Ru, D6, Auth, GID, SK, M2, SIDj, Aa, Ee, Cc, Bb: text
Const aa, bb, cc, ii, ww, sensor_user_sc,
user_sensor_sc: protocol_id
Init State: = 3
Transition
1.    State = 3 /\ RCV_SG(xor((IDi.GID'.M1'.Bb'.Ee'),S1')
      .H(IDi.GID'.M1'.Bb'.Ee'.S1')) =|>
State':= 4 /\ secret ({Xs}, aa, {GW})
            /\ secret ({PIDi}, ii, {Ui, GW})
            /\ secret ({Ru}, cc, {Ui})
            /\ secret ({IDi}, sc_user_id, {Ui})
            /\ secret ({PWi, Bioi}, bb, {Sj, GW})
            /\ secret ({SIDj}, sc_sensor_id, {Sj})
            /\ Cc':= new ()
            /\ M2':= exp (Cc'.P)
            /\ SK':= H (IDi.SIDj.GID'.exp (Cc'.M1').Ee'.Bb')
            /\ D7':= xor (S1', M2')
            /\ Auth':= H (SIDj.S1'.M2')
            /\ SND_SG (D7'.Auth')
            /\ witness (Sj, Ui, sensor_user_sc, SK')
            /\ request (Sj, Ui, user_sensor_sc, SK')
            /\ request (Sj, GW, ww, S1')

End role
```

Fig 5.4. Code HLPSL pour le rôle de Sensor

```
Role gateway (GW: agent, Ui: agent, Sj: agent,
Xi: symmetric_key,
H: hash_func,
P: text,
SND_UG, RCV_UG, SND_SG, RCV_SG: channel (dy))
Played_by Ui
Def=
Local State: nat,
PWi, IDi, Bioi, D5, Xs, Ru, D6, S0, S1, Ai: text,
D8, D9, Cc, Auth2, Knew, GID, SK, M1: text,
Bb, M2, PIDinew, B, SIDj, Aa, Ee, PIDi: text
const aa, bb, cc, ii, ww, zz, sc_user_id, sc_sensor_id: protocol_id
Init State: = 0
Transition
1. State = 0 /\ RCV_UG ({H (IDi.PWi.Ru).IDi} _Xi) =|>
State':= 1   /\ secret ({Xs}, aa, {GW})
             /\ secret ({PIDi}, ii, {Ui, GW})
             /\ secret ({Ru}, cc, {Ui})
             /\ secret ({IDi}, sc_user_id, {Ui})
             /\ secret ({PWi, Bioi}, bb, {Ui})
             /\ secret ({SIDj}, sc_sensor_id, {Sj, GW})
             /\S0':= H (Xs.IDi)
             /\S1':= H (Xs.SIDj)
             /\SND_SG ({PIDi.S0'} _Xi)
 2. State = 1 /\   RCV_UG
(PIDi.B'.xor ((SIDj.Ee'), Ai').H (IDi.xor ((SIDj.Ee'), Ai').Ai'.Ee')) =|>
 State':= 2 /\Bb':= new ()
            /\M1':= xor (B', Ai')
            /\D5':= xor ((IDi.GID.M1'.Bb'.Ee'), H (S1))
            /\D6':= H (IDi.GID.M1'.Bb'.Ee'.H (S1))
            /\SND_SG (D5'.D6')
3. State = 2 /\ RCV_SG (xor (H (S1), M2').H (SIDj.H (S1).M2')) =|>
State':= 3 /\PIDinew':= new ()
            /\D8':=xor ((GID.Bb.M2'), H (S0))
            /\D9':=xor (PIDinew', H (S0))
            /\Auth2':=H (GID.Bb. H (S0). M2'.PIDinew')
            /\SND_UG (D8'.D9'.Auth2')
            /\ witness (GW, Ui, zz, S0)
            /\ witness (GW, Sj, ww, S1)
End role
```

Fig 5.5. Code HLPSL pour le rôle de Gateway

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/z.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.48s
  visitedNodes: 20 nodes
  depth: 4 plies
```

Fig 5.6. Résultats de simulation de notre schéma sous OFMC

5.4.3 **Analyse de sécurité de solution proposée**

La sécurité du système est analysée et prouvée contre différents types d'attaques.

- **Authentification mutuelle :** Cette autorisation est accordée à chaque étape du système proposé avec une clé secrète commune initiale au stade initial de chaque entrée de données. L'utilisateur Ui et le GWN s'authentifient mutuellement en vérifiant respectivement :

  $$L3^* = L3,$$
  $$Auth2^* = Auth2.$$

  Ensuite, les dispositifs IoD's s'authentifient mutuellement avec le GWN en vérifiant respectivement :

  $$L6^* = L6,$$
  $$Auth^* = Auth.$$

  Successivement, Sj et Ui établissent une clé de session SKi en obtenant GID, b, M2 et en vérifiant Auth2*. Le schéma proposé offre une authentification mutuelle.

- **Attaque de rejeu (Replay Attack) :** Le protocole est sécurisé contre les attaques de rejeu en utilisant une méthode de numérotation aléatoire. L'utilisateur Ui, le GWN et le dispositif intelligent Sj génèrent des nombres aléatoires e, b et c. L'utilisation de ces nombres aléatoires permet de garantir que les messages étendus sont à jour et frais.

- **Attaque de vol de carte intelligente (Stolen Smart Card Attack) :** On suppose que la carte intelligente de Ui est perdue et obtenue par l'attaquant ἐ, alors ἐ peut récupérer les données {Di, Pu, PIDi, xi, Gen (.), Rep (.)} et restaurer les paires de données {IDi, Guess PWi}, mais l'information Ru est nécessaire pour que ἐ puisse vérifier la validité de la paire de données devinée à partir de Di. Cependant, ἐ ne peut pas deviner l'identité et le mot de passe de Ui à partir de Di. De plus, sans connaître Ru, en raison de la propriété à sens unique des fonctions de hachage h (•). Par conséquent, le protocole est protégé contre l'attaque de vol de carte intelligente.

- **Anonymat des utilisateurs (User Anonymity) :** Dans la demande de connexion M1 = {PIDi, B, L1, L2, L3}, le protocole agit comme un substitut de l'identité réelle. Pour obtenir l'identité de Ui à partir de L1, la clé secrète Ru et le nombre aléatoire a sont des informations nécessaires pour ἐ. Cependant, PIDi est une pseudo-identité connue uniquement par le GWN et Ui, et Ai = h (IDi || PWi || Ru), mais l'information Ru est nécessaire pour que ἐ puisse vérifier la validité de la paire de données devinée à partir de Ai, et a est une clé secrète uniquement connue par Ui. En revanche, le GWN peut obtenir IDi à partir de la demande de connexion en obtenant K en utilisant PIDi, en récupérant :

  $$Ai = K \oplus h (Xs || PIDi)$$ et en calculant :
  $$M1 = Ai \oplus B,$$
  $$IDi = L1 \oplus h (PIDi || Ai || M1).$$

  Par conséquent, le protocole atteint l'anonymat des utilisateurs et assure la vérification de l'identité de l'utilisateur.

- **L'impossibilité de traçabilité (Untraceability) :** Chaque élément de la demande de connexion change dynamiquement avec un nombre aléatoire e. Par conséquent, un attaquant ne peut pas suivre un utilisateur spécifique lorsqu'il intercepte les messages de demande de connexion, et la fonctionnalité d'anonymat est garantie.

- **Anonymat des capteurs (Sensor Anonymity) :** L'identité SIDj de l'appareil IdO n'est pas transmise via le canal public, et le GWN peut récupérer le SIDj à partir de la demande de connexion en comptant :

$$Ai=Ki\oplus h(Xs||PIDi),$$
$$M1=Ai\oplus B,$$
$$IDi=L1\oplus h(PIDi||Ai||M1),$$
$$\text{Récupérer } SIDj\oplus e=L2\oplus Ai.$$

  Par conséquent, le protocole garantit l'anonymat du nœud capteur.
- **Protection du modèle biométrique (Protection of Biometric Template):** Le modèle biométrique BIOi de Ui est protégé par un extracteur flou Gen (BIOi) = (RU, PU), où RU est protégé par la propriété à sens unique de la fonction de hachage h (•). Par conséquent, le protocole protège le modèle biométrique.

- **Attaque privilégiée par un initié (Privileged-insider Attack):** L'administrateur réseau ou l'administrateur système peut accéder à la clé secrète de l'utilisateur pour mener une attaque d'insider. Un adversaire ἐ, un utilisateur privilégié au GWN, a accès aux informations d'enregistrement de Ui. Supposons que la carte à puce SC de Ui soit volée par ἐ après l'enregistrement. Même avec accès à tous les détails stockés dans SC tels que {Di, Pu, PIDi, xi, Gen (.), Rep (.)}, ἐ ne peut deviner ni IDi ni PWi lorsque Ui s'enregistre auprès du GWN dans notre schéma. Ui envoie le message de demande d'enregistrement {IDi, Ai} à GWN. Un adversaire ne peut pas obtenir le mot de passe PWi de Ui à partir de Ai car il est protégé par les valeurs IDi, RU est nécessaire, et la propriété à sens unique de la fonction de hachage h (•) protège ces données. En conclusion, le schéma proposé est sécurisé contre cette attaque.

- **Attaque de Devinette de Mot de Passe Hors Ligne (Offline Password Guessing Attack) :** En supposant qu'un adversaire ἐ ait accès à toutes les informations sensibles de la carte intelligente SC de Ui, qui sont {Di, Pu, PIDi, xi, Gen (.), Rep (.)}, il est impossible pour ἐ de calculer le mot de passe PWi de Ui en raison de la propriété unidirectionnelle de la fonction de hachage h (•), qui cache les valeurs IDi et Ru à partir de Ai. Par conséquent, le schéma est protégé contre cette attaque.

- **Confidentialité à Avancement (Forward Secrecy) :** Dans le schéma proposé, le Ski contient les nombres aléatoires e, b, c et les IDi, GID, SIDj, c•M1=c•a•G. Ainsi, il ne peut pas être compromis par un attaquant ἐ sans connaître les nombres aléatoires e, b, c et les IDi, GID, SIDj, c•M1. Cela n'affecte pas la confidentialité des communications précédentes. Par conséquent, cela n'aide pas ἐ à calculer les clés de session futures dans le schéma proposé.

- **Attaques d'usurpation d'Identité (Impersonation Attacks):** Supposons que l'adversaire ἐ essaie de se faire passer pour un utilisateur Ui en falsifiant un message de demande de connexion valide Mes1 = {PIDi, B, L1, L2, L3}, ἐ doit connaître IDi et Ai = h (IDi||PWi||Ru). Cependant, ἐ ne peut pas se faire passer pour l'identité Ui et ne peut pas obtenir d'informations à partir de la carte intelligente de l'utilisateur. De plus, notre schéma peut résister à l'attaque d'usurpation d'utilisateur. De plus, dans notre protocole, ἐ ne peut pas se faire passer pour un GWN sans connaître Xs, qui est détenu uniquement par le GWN. De plus, ἐ ne peut pas obtenir SIDj avec L7 = xj⊕M2, lorsque M2 = c•G. Ainsi, le schéma suggéré peut résister à l'attaque d'usurpation du capteur.

- **Homme du Milieu (Man in the Middle):** Cette attaque est une véritable menace pour les architectures distribuées ou centralisées mentionnées dans plusieurs travaux (Zakariae et al., 2020). Le protocole peut fournir une authentification mutuelle réussie. Les valeurs secrètes Ai, M1, xj, xi protègent les messages transmis entre l'utilisateur et la passerelle/la passerelle et l'appareil IdO, et vice versa. Ainsi, le système est résistant à cette attaque.

- **Détection des connexions non autorisées (Detection for Unauthorized Login) :** Elle repose sur trois facteurs. L'utilisateur Ui insère la carte intelligente (SC) dans le lecteur, entre son identité et son mot de passe, imprime les informations biométriques BIOi' sur l'appareil mobile et calcule Ru = Rep (BIOi', Pu). Ensuite, il vérifie si les données biométriques, l'identité et le mot de passe sont valides en calculant :

  Di* = h (IDi || h (Ru) || PWi),

  Et vérifie si Di* ? = Di.

  Ainsi, l'utilisateur peut accéder au système, et le schéma peut détecter les connexions non autorisées.

- **Attaque de désynchronisation (De-synchronization Attack) :** Dans cette approche, les attaques de désynchronisation sont impossibles, car il n'est pas nécessaire de mettre à jour les informations une fois qu'une session est terminée.
- **Établissement de la clé de session :** Dans cette méthode, la clé de session est calculée comme suit :

  SKi = h (IDi || SIDj || GID || aM2 || e || b) = h (IDi || SIDj || GID || a•c•G || e || b),

  À partir de la clé de session partagée SKi qui peut uniquement être calculée par Ui et Sj. Par conséquent, il est impossible d'obtenir Ski sans connaître les valeurs aléatoires a, b, c, e et l'identité de l'utilisateur, du dispositif capteur et du réseau sans fil global (GWN). Le schéma proposé permet une réussite dans l'établissement des clés de session.

5.4.4 Comparaison des Fonctionnalités de Sécurité

Dans cette section, le Tableau 5.6 présente la comparaison et l'évaluation de l'approche proposée avec d'autres protocoles similaires [40], [51], [85] en termes de fonctionnalités de sécurité. De plus, le schéma proposé offre une sécurité supérieure aux schémas de [40], [51], [85].

Attaques	[40]	[51]	[85]	Notre protocole
Mutual authentication	Yes	Yes	Yes	Yes
Session key agreement	Yes	Yes	Yes	Yes
User/Sensor anonymity	No	Yes	Yes	Yes
Untraceability	No	Yes	Yes	Yes
Freely password change	Yes	Yes	Yes	Yes
Detection mechanism for unauthorized login	Yes	No	Yes	Yes
Suitable for IdO environments	No	Yes	Yes	Yes
Resistant to replay attack	Yes	No	Yes	Yes
Resistant to stolen smart card attack	No	No	Yes	Yes
Resistant to session-specific temporary information attack	No	No	No	Yes
Resist impersonation attack	Yes	No	Yes	Yes
Avoid of clock synchronization problem	Yes	Yes	Yes	Yes
Forward secrecy	No	No	Yes	Yes
Insider attack	Yes	No	Yes	Yes
Dos attack	No	No	No	Yes
Man-in-the-Middle	Yes	No	No	Yes

Tab 5.6. Comparaison en termes de fonctionnalités et de caractéristiques de sécurité

5.5 ÉVALUATION DES PERFORMANCES ET ANALYSE DE LA DISCUSSION

Les coûts de calcul et de communication du schéma proposé sont comparés aux schémas de [40], [51], [85], et les résultats sont présentés dans le Tableau 5.7 et le Tableau 5.8.

5.5.1 Coût de communication

Pour comparer les coûts de communication, on suppose que l'ECC, le hachage (en supposant l'application de "SHA-2") et les identités des utilisateurs, l'identité du capteur, l'identité arbitraire de l'utilisateur alias et le chiffrement symétrique sont respectivement de 320 bits, 160 bits, 128 bits, 128 bits, 160 bits, 128 bits et 160 bits. Au cours de la phase de connexion et d'authentification, le schéma proposé échange quatre messages qui sont {PIDi, B, L1, L2, L3}, {L5, L6}, {L7, Auth} et {L8, L9, Auth2}, nécessitant respectivement (128 + 160 + 128 + 160 + 160) = 736 bits, (160 + 160) = 320 bits, (160 + 160) = 320 bits et (160 + 160 + 160) = 480 bits. Le Tableau 6.5 liste la comparaison du coût total de communication entre le schéma proposé et les schémas de [40], [51], [85], qui sont respectivement de 1696 bits, 3072 bits, 3168 bits et 2720 bits. Comme le montre la Figure 5.7, le coût de communication du schéma proposé est plus efficace que les schémas de [40], [51], [85].

5.5.2 **Coût de calcul**

Le coût de calcul total du schéma proposé et des schémas de [40], [51], [85]est respectivement de 15TH+4TM et 19TH+6TM, 17TH+4TM et 19TH+6TM, où TM et TH sont définis comme le coût temporel d'une opération de multiplication scalaire et d'une opération de fonction de hachage. De plus, le Tableau 5.9 présente le coût de calcul de chaque entité dans le protocole proposé, et le Tableau 5.8 montre que le coût de calcul du schéma proposé est légèrement plus élevé que celui des schémas de [40], [51], [85].

	Nombre total de messages	***Coût de communication* (bits)**
[40]	4 Messages	3072 bits
[51]	4 Messages	3168 bits
[85]	4 Messages	2720 bits
Notre schéma	4 Messages	1856 bits

Tab 5.7. Coût de communication par rapport aux protocoles existants

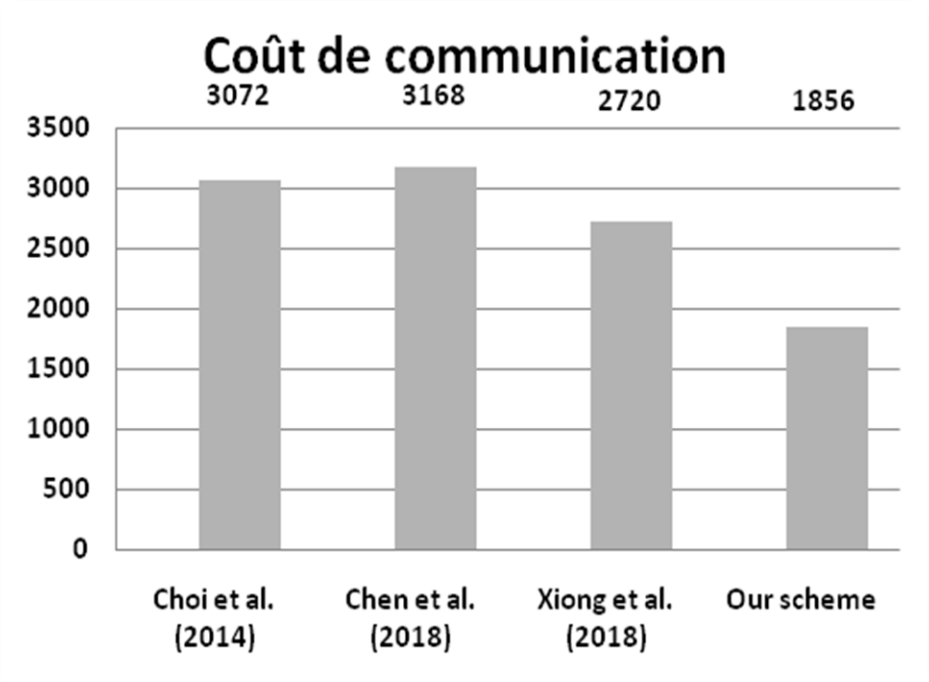

Fig 5.7. Coût de communication

Protocoles	Sj's nœud	Ui's nœud	GWN's nœud	Coût total
[40]	2TM + 5TH	3TM + 9TH	1TM + 5TH	6TM + 19TH
[51]	4TH + 2TM	5TH +2TM	8TH	17TH + 4TM
[85]	4TH+2TM	8TH+3TM	7TH+TM	19TH+6TM
Notre schéma	3TH+2TM	7TH+2TM	5TH	15TH+4TM

Tab 5.8. Coût de calcul par rapport aux protocoles existants

Nœud	*Coût de calcul*
Ui nœud	7TH+2TM
Sj	3TH+2TM
GWN	5TH
Coût total	15TH+4TM

Tab 5.9. Coût de calcul de notre protocole

8.1 **CONCLUSION**

Dans ce chapitre, nous avons proposé un schéma d'authentification avec confidentialité et établissement de clé pour l'IdO utilisant ECC, la biométrie et Fuzzy Extractor afin de garantir l'anonymat des utilisateurs/capteurs, l'impossibilité de les tracer et la confidentialité avancée. L'approche proposée s'est révélée sécurisée en résistant à de nombreuses attaques telles que l'attaque privilégiée de l'insider, l'attaque de devinette de mot de passe hors ligne et l'attaque de vol de carte intelligente. Nous avons ensuite utilisé un modèle logique largement accepté, le modèle Burrows-Abadi-Needham (BAN), pour démontrer la sécurité, l'authentification mutuelle et l'établissement réussi de la clé de session entre l'utilisateur (Ui) et le dispositif IdO (Sj) en utilisant la passerelle (GWN).

De plus, l'analyse des performances de la méthode proposée comparée à d'autres travaux connexes a montré que cette approche est à la fois fiable et sécurisée. Par conséquent, le schéma proposé est convivial pour les utilisateurs et adapté aux environnements IdO.

CONCLUSION GENERALE ET PERSPECTIVES

Conclusion Générale et Perspectives

Dans le contexte de l'Internet des objets (IdO), la croissance exponentielle du partage de données personnelles et physiologiques des utilisateurs avec des entités distantes intensifie le risque de violations de la vie privée. Ainsi, la gestion sécurisée de l'accès aux données devient impérative.

Nous proposons, dans cette thèse, trois contributions majeures dans le domaine de la sécurité et de l'authentification pour l'Internet des objets (IdO). Notre première proposition introduit une approche novatrice garantissant la confidentialité, l'intégrité, l'authentification de l'utilisateur et la préservation de la vie privée. Deux types de clés basées sur les courbes elliptiques (ECDH) et L'infrastructure à clé publique (PKI) sont présentés : les clés certifiées à long terme, liées à l'identité, et les Alias anonymes temporaires, générés de manière dynamique.

Notre deuxième proposition présente un système d'authentification performant en termes de sécurité, de coûts de calcul et de communication. Ce protocole vise à sécuriser les informations des capteurs IdO lors de leur diffusion et de leur sauvegarde en utilisant le chiffrement ECC pour la protection des données et le Fuzzy Extractor pour l'authentification de l'utilisateur.

Enfin, notre dernier chapitre se concentre sur la multiplication scalaire sur les courbes elliptiques, l'opération fondamentale de tous les protocoles reposant sur ces objets mathématiques. Nous proposons une nouvelle méthode d'authentification et d'échange de clés pour l'IdO en utilisant l'algorithme ECC et un extracteur flou, visant à garantir la sécurité des données transmises et stockées par les capteurs de l'IdO tout en minimisant les coûts. Ces contributions offrent des avancées significatives pour renforcer la sécurité et la confidentialité des systèmes IdO.

L'analyse des performances que nous proposons a démontré l'efficacité et la robustesse des méthodes présentées dans cette thèse par rapport aux travaux connexes en termes de coûts. Pour la première contribution, la gestion des clés certifiées à long terme et des Alias anonymes temporaires que nous proposons a été évaluée, mettant en lumière une gestion fluide et sécurisée des identités dans le contexte de l'IdO. Les résultats ont montré une diminution significative des risques liés à la vie privée tout en permettant une authentification fiable des utilisateurs.

Pour les deuxième et troisième contributions, les performances du nouveau système d'authentification que nous proposons ont été évaluées en termes de sécurité, de coûts de calcul et de communication. Les tests ont révélé une réduction notable des coûts opérationnels sans compromettre la sécurité des informations des capteurs IdO. Les protocoles que nous proposons ont démontré une résistance robuste contre les attaques potentielles, assurant ainsi l'intégrité des données tout au long du processus de transmission et de stockage.

En conclusion, l'analyse globale des performances que nous proposons valide la pertinence et l'applicabilité pratique des contributions de cette thèse dans le contexte dynamique et complexe de l'Internet des objets. Les résultats obtenus renforcent la crédibilité des méthodes que nous

proposons et ouvrent la voie à leur intégration potentielle dans des applications concrètes, offrant ainsi des solutions fiables pour garantir la sécurité des données dans les environnements IdO.

Comme perspective, nous envisageons d'explorer l'incidence de l'utilisation de la technologie blockchain sur nos propositions, en mettant l'accent sur le temps de calcules et de communications. Nous avons pour objectif d'incorporer d'autres techniques cryptographiques dans le mécanisme d'authentification afin de simplifier le processus d'authentification et de l'adapter aux nouvelles générations des réseaux, tels que la 5G, 6G. Possibilité d'intégration de L'IA dans le domaine IoT.

RÉFÉRENCES

[1] Evans, "Cisco Internet Business Solutions Group (IBSG) The Internet of Things How the Next Evolution of the Internet Is Changing Everything," Apr. 2011. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," *Gartner*, 2017. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[3] Nasreddine Bouhaï and I. Saleh, *Internet des objets : évolutions et innovations*. Londres, Uk: Iste Editions, 2017.

[4] "L'IdO et la chaîne d'approvisionnement : comment l'apprentissage automatique élimine les bouchons," *fr.digi.com*. https://fr.digi.com/blog/post/iot-supply-chain (accessed Apr. 12, 2024).

[5] "Thèse de Mohamad Fardon," *Laboratoire d'InfoRmatique en Image et Systèmes d'information*, Dec. 23, 2017. https://liris.cnrs.fr/these/these-mohamad-fardon (accessed Apr. 12, 2024).

[6] L. Atzori, A. Lera, et G. Morabioto, "The Internet of Things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[7] J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey," *Ad Hoc Networks*, vol. 24, pp. 264–287, Jan. 2015, doi: https://doi.org/10.1016/j.adhoc.2014.08.001.

[8] M. De Béjaïa, "République Algérienne Démocratique et Populaire Ministère de l'Enseignement Supérieur et de la Recherche Scientique." Accessed: Apr. 12, 2024. [Online]. Available: https://www.univ-bejaia.dz/jspui/bitstream/123456789/8582/1/proposition%20d%27un%20mod%C3%A8le%20de%20confiance%20pour%20l%27Internet%20des%20Objets_elhamdoulilah.pdf

[9] F. Abbas and U. Setif, "PEOPLEs' DEMOCRATIC REPUBLIC of ALGERIA Ministry of Higher Education and Scientific Research." Accessed: Apr. 12, 2024. [Online]. Available: http://dspace.univsetif.dz:8888/jspui/bitstream/123456789/3759/1/ThesisYasmineHARBI.pdf

[10] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: https://doi.org/10.1109/jiot.2017.2694844.

[11] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–29, Jan. 2019, doi: https://doi.org/10.1145/3292674.

[12] D. Team, "4 Key IoT Protocols - Learn In Great Detail," *DataFlair*, Jun. 18, 2018. https://data-flair.training/blogs/iot-protocols/

[13] A. Bashir and A. H. Mir, "Securing Publish-Subscribe Services with Dynamic Security Protocol in MQTT Enabled Internet of Things," *International Journal of Security and Its Applications*, vol. 11, no. 11, pp. 53–66, Nov. 2017, doi: https://doi.org/10.14257/ijsia.2017.11.11.05.

[14] "28 PDF | PDF | Internet des objets | l'Internet," *Scribd*. https://fr.scribd.com/document/644779777/28-pdf (accessed Apr. 12, 2024).

[15] "Comment la RFID et l'Internet des objets sont-ils liés ? - WXR," *https://www.rfidfuture.com/fr*. https://www.rfidfuture.com/fr/rfid-and-the-internet-of-things.html (accessed Apr. 12, 2024).

[16] F. Sureau, *Un système de composants distribué pour les réseaux de capteurs sans-fils*. Université de Sherbrooke, 2011. Accessed: Apr. 12, 2024. [Online]. Available: http://savoirs.usherbrooke.ca/handle/11143/1597

[17] "CERIST (Centre de Recherche sur l'Information Scientifique et Technique) - CERIST," *www.cerist.dz*. https://www.cerist.dz/doc/PNR/valorise/MISE_EN_PLACE_RESEAU_DE_CAPTEUCA_SANS_FIL_FORET.pdf (accessed Apr. 12, 2024).

[18] "4 different Definitions of Cybersecurity from NIST," *Security Scientist*, Feb. 07, 2022. https://www.securityscientist.net/blog/the-definition-of-cybersecurity-according-to-nist/

[19] A. N. Soni, "Security Challenges and Future Applications of Smart Devices Based on Internet of Things," *SSRN Electronic Journal*, 2020, doi: https://doi.org/10.2139/ssrn.3761340.

[20] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," in *IEEE Network*, vol. 33, no. 2, pp. 82-88, March/April 2019, doi: 10.1109/MNET.2019.1800240.

[21] S. Singh, “Multi-factor Authentication and their Approaches,” *International Research Journal of Management, IT and Social Sciences*, May 2017, doi: https://doi.org/10.21744/irjmis.v4i3.464.

[22] “Définition Cryptographie,” *Actualité Informatique*, Jan. 16, 2021. https://actualiteinformatique.fr/cryptomonnaie/definition-cryptographie. (accessed Apr. 12, 2024).

[23] “Cryptographie : définition et explications,” *Techno-Science.net*. https://www.techno-science.net/definition/6154.html (accessed Apr. 12, 2024).

[24] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, *Guide to elliptic curve cryptography*. New York ; London: Springer, 2011.

[25] “ÉPREUVE COMMUNE DE TIPE 2008 -Partie D TITRE : Les Fonctions de Hachage.” Accessed: Apr. 12, 2024.[Online]. Available:https://www.chireux.fr/mp/TIPE/ADS/fonctions%20de%20hachage.pdf

[26] “Certificats d’appareils IoT,” *GlobalSign*, Nov. 29, 2022. https://www.globalsign.com/fr/internet-des-objets/certificats-appareils-iot (accessed Apr. 12, 2024).

[27] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.1,” vol. 4346, pp. 1–87, Apr. 2006.

[28] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," *2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, China, 2012, pp. 648-651, doi: 10.1109/ICCSEE.2012.373.

[29] L. Chen *et al.*, “Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey,” *IEEE Access*, vol. 5, pp. 8956–8977, 2017, doi: https://doi.org/10.1109/ACCESS.2017.2695525.

[30] M. Shuai, N. Yu, H. Wang, and L. Xiong, “Anonymous authentication scheme for smart home environment with provable security,” *Computers & Security*, vol. 86, pp. 132–146, Sep. 2019, doi: https://doi.org/10.1016/j.cose.2019.06.002.

[31] P. K. Dhillon and S. Kalra, “Secure multi-factor remote user authentication scheme for Internet of Things environments,” *International Journal of Communication Systems*, vol. 30, no. 16, p. e3323, Apr. 2017, doi: https://doi.org/10.1002/dac.3323.

[32] R. Dojen, A. Jurcut, T. Coffey, & C. Gyorodi, “On Establishing and Fixing a Parallel Session Attack in a Security Protocol,” In C. Badica, G. Mangioni, V. Carchiolo, D. D.

Burdescu (Eds.), *Intelligent Distributed Computing, Systems and Applications, Springer*, pp. 239-244, 2008.

[33] S. Tu *et al.*, "Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack," *IEEE Access*, vol. 6, pp. 74993–75001, 2018, doi: https://doi.org/10.1109/ACCESS.2018.2884672.

[34] A. D. Jurcut, T. Coffey, and Reiner Dojen, "Design requirements to counter parallel session attacks in security protocols," Jul. 2014, doi: https://doi.org/10.1109/pst.2014.6890952.

[35] J. Jeong, M. Y. Chung, and H. Choo, "Integrated OTP-Based User Authentication Scheme Using Smart Cards in Home Networks," *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, Jan. 2008, doi: https://doi.org/10.1109/hicss.2008.208.

[36] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009, doi: https://doi.org/10.1109/TWC.2008.080128.

[37] M. K. Khan and K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, Mar. 2010, doi: https://doi.org/10.3390/s100302450.

[38] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, May 2011, doi: https://doi.org/10.3390/s110504767.

[39] W. Shi and P. Gong, "A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, p. 730831, Jan. 2013, doi: https://doi.org/10.1155/2013/730831.

[40] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, Jun. 2014, doi: https://doi.org/10.3390/s140610081.

[41] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the Security: An ECC-Based Authentication Scheme for Internet of

Drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021, doi: https://doi.org/10.1109/JSYST.2021.3057047.

[42] M. Zhang, C. Xu, S. Li, & C. Jiang, "On the Security of an ECC-Based Authentication Scheme for Internet of Drones," *in IEEE Systems Journal*, 2022, doi: 10.1109/JSYST.2022.3162604.

[43] [43] T. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks," *Drones*, vol. 6, no. 1, p. 10, Dec. 2021, doi: https://doi.org/10.3390/drones6010010.

[44] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: https://doi.org/10.1016/j.comnet.2012.12.018.

[45] Q. Zhu, Q. Zhang, & Y. Chen, "Decentralized Access Control and Authentication Protocol for the Internet of Things," *IEEE Transactions on Industrial Informatics*, 14(2), 656-667, 2018.

[46] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based Decentralized Authentication Modeling Scheme in Edge and IoT Environment," *IEEE Internet of Things Journal*, pp. 1–1, 2020, doi: https://doi.org/10.1109/jiot.2020.3037733.

[47] H. Zhao, X. Zhang, Y. Wang, W. Wang, & H. Zhu, "A Decentralized and Distributed IoT Authentication Protocol Based on Smart Contracts," *IEEE Internet of Things Journal*, 8(14), 12005-12016, (2021).

[48] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, Sep. 2014, doi: https://doi.org/10.1016/j.adhoc.2014.03.009.

[49] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, Jan. 2016, doi: https://doi.org/10.1016/j.adhoc.2015.05.014.

[50] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269-282, Feb. 2018, doi: 10.1109/JIOT.2017.2780232.

[51] Y. Chen, L. López, J.-F. Martínez, et P. Castillejo, “A Lightweight Privacy Protection User Authentication and Key Agreement Scheme Tailored for the Internet of Things Environment: LightPriAuth,” *Journal of Sensors*, vol. 2018, pp. 1–16, 2018.

[52] A. Sebbah et B. Kadri, “A Privacy and Authentication Scheme for IoT Environments Using ECC and Fuzzy Extractor,” *in 2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, 2020, pp. 1-5.

[53] A. Gupta, M. Tripathi, T. J. Shaikh, et A. Sharma, “A Lightweight Anonymous User Authentication and Key Establishment Scheme for Wearable Devices,” *Computer Networks*, 2018.

[54] Y. Zhou, T. Liu, F. Tang, et M. Tinashe, “An unlinkable authentication scheme for distributed IoT application,” *IEEE Access*, vol. 1, pp. 1–1, 2019.

[55] A. Sebbah et B. Kadri, “Security Issues in the Internet of Things,” *in International Conference on Managing Business Through Web Analytics*, S. Sedkaoui, M. Khelfaoui, R. Benaichouba, et K. Mohammed Belkebir, Eds. Springer, 2022, DOI: 10.1007/978-3-031-06971-0_16.

[56] L. Benarous et B. Kadri, “The quest of privacy in public key infrastructure,” *International Journal of Blockchains and Cryptocurrencies*, vol. 2, no. 3, 2021.

[57] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, et Y. Park, “Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges,” *IEEE Access*, vol. 8, pp. 3343-3363, 2020, doi: 10.1109/ACCESS.2019.2962829.

[58] A. A. Ahmed, S. J. Malebary, W. Ali, et A. A. Alzahrani, “A provable secure cybersecurity mechanism based on a combination of lightweight cryptography and authentication for the Internet of Things,” *Mathematics*, vol. 11, no. 1, p. 220, 2023, https://doi.org/10.3390/math11010220.

[59] A. A. Ahmed et W. A. Ahmed, “An effective multifactor authentication mechanism based on combiners of hash function over the Internet of Things,” *Sensors*, vol. 19, p. 366, 2019.

[60] B. Kadri, M. Benamar, M. Feham, et A. M'Hamed, “Lightweight PKI for WSNs uPKI,” *International Journal of Network Security*, vol. 10, 2010.

[61] Chandrashekhar Meshram and Shyam Sundar Agrawal, “An ID-Based Public Key Cryptosystem based on Integer Factoring and Double Discrete Logarithm Problem,” *Jan.* 2010.

[62] D. Boneh et M. Franklin, “Identity-based encryption from the Weil pairing,” *in Annual International Cryptology Conference*, 2001, pp. 213–229.

[63] S. S. Al-Riyami et K. G. “Paterson, Certificateless public key cryptography, ” *in International Conference on the Theory and Application of Cryptology and Information Security*, 2003, pp. 452–473.

[64] C. Adams et S. Farrell, “RFC2510: Internet X.509 Public Key Infrastructure Certificate Management Protocols, ” *RFC Editor*, USA, 1999.

[65] C. Ellison et al., “Ten risks of PKI: What you’re not being told about public key infrastructure, ” *Comput. Secur. J.*, 2000.

[66] J. Zhu, C. Wan, P. Nie, Y. Chen, et Z. Su, “Guided, Deep Testing of X.509 Certificate Validation via Coverage Transfer Graphs,” *in IEEE*, 2020, pp. 243–254.

[67] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain Technologies for the Internet of Things: Research Issues and Challenges,” *IEEE Internet of Things Journal*, pp. 1–1, 2018, doi: https://doi.org/10.1109/jiot.2018.2882794.

[68] J. Shi, X. Zeng, and R. Han, “A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks,” *Information*, vol. 13, no. 5, p. 264, May 2022, doi: https://doi.org/10.3390/info13050264.

[69] M. Patel, “The Security and Privacy of Wearable Health and Fitness Devices,” *Security Intelligence*, Sep. 10, 2015. https://securityintelligence.com/the-security-and-privacy-of-wearable-health-and-fitness-devices. (accessed Apr. 12, 2024).

[70] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: https://doi.org/10.1016/j.comnet.2014.11.008.

[71] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: https://doi.org/10.1109/jiot.2017.2694844.

[72] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: https://doi.org/10.1109/jiot.2017.2683200.

[73] V. Morgante, “PKI : Qu’est-ce qu’une PKI ou Infrastructure à clés publiques ?,” *Certeurope*, Jul. 26, 2022. https://www.certeurope.fr/blog/quest-ce-quune-pki-ou-infrastructure-a-cles-publiques (accessed Apr. 12, 2024)

[74] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987, doi: https://doi.org/10.1090/S0025-5718-1987-0866109-5.

[75] V. S. Miller, "Use of elliptic curves in cryptography," *in Lecture Notes in Computer Sciences, on Advances in cryptology—CRYPTO 85, Springer-Verlag*, New York, NY, USA, 1986, vol. 218, pp. 417–426.3, doi: https://doi.org/10.1109/tit.1983.1056650.

[76] O. Rafik and F. Mohammed, “The impact of ECC’s scalar multiplication on wireless sensor networks,” Apr. 2013, doi: https://doi.org/10.1109/isps.2013.6581488.

[77] “What is the Elliptic-curve Diffie-Hellman algorithm?,” *Educative: Interactive Courses for Software Developers*. https://www.educative.io/answers/what-is-the-elliptic-curve-diffie-hellman-algorithm

[78] “Elliptic Curve Cryptography for dummies 2: en pratique pour la cryptographie | Smals Research,” *www.smalsresearch.be*. https://www.smalsresearch.be/elliptic-curve-cryptography-tutoriel2/

[79] “Botnet : Mirai, DDoS… quelles sont les attaques contre l’IoT ?,” *www.journaldunet.fr*, Jul. 19, 2021. https://www.journaldunet.fr/web-tech/dictionnaire-de-l-IdO/1440656-botnet-mirai-ddos-les-attaques-contre-l-iot-20200414/ (accessed Apr. 12, 2024).

[80] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, “A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018, doi: https://doi.org/10.1109/TII.2017.2773666.

[81] Y. Lu, L. Li, H. Peng, et Y. Yang, "A secure and efficient mutual authentication scheme for session initiation protocol," *Peer-to Peer Netw Appl*, vol. 9, no. 2, pp. 449–459, 2016.

[82] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, et K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018. https://doi: 10.1016/j.jnca.2017.07.001

[83] Khwaja Jawad, Khwaja Mansoor, Ahmed Fraz Baig, Anwar Ghani, et Azmat Naseem, "An Improved three-factor anonymous Authentication Protocol for WSNs based IdO System Using Symmetric cryptography," *International Conference on Communication Technologies*, 2019.

[84] Y. Dodis, R. Ostrovsky, L. Reyzin, et A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, ” *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

[85] José M. Sierra, Julio C. Hernández, Almudena Alcaide, et Joaquín Torres, “Validating the Use of BAN LOGIC, ” *in Computational Science and Its Applications - ICCSA 2004, International Conference, Assisi, Italy*, 2004, 14-17.

[86] M. Burrows, M. Abadi, and R. Needham, “A logic of authentication,” *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, Feb. 1990, doi: https://doi.org/10.1145/77648.77649.

[87] Y. Park, K. Park, and Y. Park, “Secure user authentication scheme with novel server mutual verification for multiserver environments,” *International Journal of Communication Systems*, vol. 32, no. 7, p. e3929, Feb. 2019, doi: https://doi.org/10.1002/dac.3929.

[88] A. Armando et al., "The AVISPA tool for the automated validation of internet security protocols and applications," *in International conference on computer aided verification, Springer, Berlin, Heidelberg*, 2005, pp. 281-285.

[89] L. Viganò, “Automated Security Protocol Analysis With the AVISPA Tool,” *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, May 2006, doi: https://doi.org/10.1016/j.entcs.2005.11.052.

[90] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, Mar. 198