



N° d'ordre : 1275 FSE /UAMOB/2026

MEMOIRE DE FIN DE CYCLE

EN VUE DE L'OBTENTION DU DIPLOME MASTER

Domaine : Mathématiques et informatique

Filière : Informatique

Spécialité : Génie des systèmes informatiques

Présenté par

Zeggane Yasmin & Rahmi Samia

Thème

startup : Un protocole d'authentification léger pour les systèmes IoT contraints
en ressources

Soutenue publiquement le : / / 2026 Devant le jury composé de :

Dr Bal Kamal

Président

Univ. Bouira

Dr Oukas Noureddine

Promoteur

Univ. Bouira

.....

co-promoteur

Univ.

.....

Examineur

Univ. Bouira

Année Universitaire (2025/2026)

Remerciements

Nous souhaitons en premier lieu remercier **ALLAH** le Tout-Puissant, qui nous a accordé la force, la patience et la volonté nécessaires pour mener à bien ce modeste travail et surmonter toutes les difficultés rencontrées durant sa réalisation.

Nous tenons ensuite à exprimer notre profonde gratitude à notre encadrant, Monsieur **Oukas Noureddine**, pour son accompagnement, sa disponibilité, ses précieux conseils ainsi que pour son soutien tout au long de ce projet.

Nous adressons également nos sincères remerciements à Madame **Sarah Boudref** pour son aide précieuse, son soutien constant et son accompagnement durant toute la période de stage.

Nos remerciements vont également à Monsieur **Nedjari** pour son aide, sa disponibilité ainsi que pour les informations et les connaissances qu'il nous a fournies, contribuant ainsi à l'avancement de notre travail.

Nous remercions chaleureusement les membres du jury pour l'honneur qu'ils nous font en acceptant d'évaluer ce travail et pour leurs remarques et suggestions qui permettront de l'enrichir.

Enfin, nous tenons à remercier toutes les personnes qui nous ont soutenues et encouragées, de près ou de loin, et qui ont contribué à l'aboutissement de ce travail.

Dédicace

À mes très chers parents

En témoignage de mon profond amour et de ma sincère gratitude pour tous les sacrifices que vous avez consentis afin de me permettre d'atteindre mes objectifs. Merci pour votre amour, votre soutien, vos conseils et vos encouragements qui m'ont accompagnée tout au long de mon parcours. J'espère que ce travail sera pour vous un motif de fierté et une modeste récompense de vos efforts.

À mes chers frères Firas, Djalil, Ikram et Zaki

Pour votre affection, votre soutien et vos encouragements tout au long de mon parcours. Merci pour votre présence à mes côtés. Je vous souhaite beaucoup de bonheur et de réussite.

À mon binôme Samia

Avec qui j'ai partagé cette belle aventure académique. Merci pour ton sérieux, ton soutien et cette agréable collaboration. Je te souhaite beaucoup de succès dans ton parcours futur.

À mes chères copines

Pour leur amitié sincère, leur soutien et tous les beaux souvenirs que nous avons construits ensemble.

À une personne chère

Pour son écoute attentive, sa bienveillance, son soutien constant et ses précieux encouragements qui m'ont donné la force de persévérer dans les moments les plus difficiles. Qu'elle trouve ici l'expression de toute ma reconnaissance, de mon estime et de ma profonde gratitude.

Enfin, à toutes les personnes qui ont contribué, de près ou de loin, à l'aboutissement de ce mémoire.

Zeggane Yasmine.

Dédicaces

C'est avec une profonde gratitude et une immense émotion que je dédie ce mémoire à :

À mes très chers parents,

Aucune dédicace ne saurait exprimer toute la gratitude, l'amour et le respect que je vous porte. Merci pour votre bienveillance, votre affection, vos sacrifices et votre soutien inconditionnel tout au long de mon parcours. Vous avez toujours été ma source de courage et de motivation. Que Dieu vous protège et vous accorde santé, bonheur et longue vie.

À mes chers frères, Samir, Nadir et Sid Ahmed,

En témoignage de mon affection et de ma reconnaissance pour votre soutien constant, votre confiance en mes capacités, vos encouragements et votre présence à mes côtés dans les moments les plus importants.

À mon binôme Yasmine,

Avec qui j'ai partagé cette belle expérience académique, les efforts, les défis et les moments de réussite. Merci pour ta collaboration, ton sérieux, ton esprit d'équipe et ton soutien tout au long de la réalisation de ce projet.

À mes chères collègues,

Pour leur aide précieuse, leur soutien moral et les agréables moments de partage durant l'élaboration de ce travail de fin d'études.

À une personne qui m'est particulièrement chère,

Pour son soutien indéfectible, sa confiance en moi, ses encouragements permanents et sa présence dans les moments difficiles.

Enfin, à tous ceux qui ont contribué, de près ou de loin, à la réalisation de ce travail, je dédie ce mémoire avec mes plus sincères remerciements.

Rahmi Samia.

Résumé

Avec le développement de l'IoT, la sécurisation des communications entre les objets connectés est devenue un enjeu majeur, notamment en raison de leurs ressources limitées. Ce mémoire propose un protocole d'authentification léger destiné aux systèmes IoT contraints, en prenant comme cas d'étude les compteurs intelligents.

Le protocole repose sur une authentification mutuelle entre le compteur intelligent et la plateforme de supervision, utilisant des fonctions de hachage, des nonces et un code OTP transmis via le service Telegram afin de garantir l'authenticité des échanges et de renforcer la cybersécurité.

Une implémentation expérimentale basée sur une carte ESP32, une plateforme développée sous VS Code et une base de données a permis de valider le bon fonctionnement du protocole. Les résultats obtenus montrent son efficacité face aux principales attaques, telles que les attaques par replay et l'usurpation d'identité.

Enfin, une étude financière prévisionnelle a montré que le projet est techniquement réalisable et économiquement viable, ce qui en fait une solution adaptée à la sécurisation des systèmes de comptage intelligents.

Mots-clés : IoT, authentification légère, compteur intelligent, cybersécurité, OTP, Telegram.

Abstract

With the development of IoT, securing communications between connected objects has become a major challenge, particularly due to their limited resources. This thesis proposes a lightweight authentication protocol for resource-constrained IoT systems, using smart meters as a case study.

The protocol relies on mutual authentication between the smart meter and the monitoring platform, using hash functions, nonces, and an OTP code transmitted via the Telegram service to guarantee the authenticity of exchanges and enhance cybersecurity.

An experimental implementation based on an ESP32 board, a platform developed using VS Code, and a database validated the protocol's functionality. The results demonstrate its effectiveness against major attacks, such as replay attacks and identity spoofing.

Finally, a preliminary financial analysis showed that the project is technically feasible and economically viable, making it a suitable solution for securing smart metering systems.

Keywords : IoT, lightweight authentication, Smart Meter, cybersecurity, OTP, Telegram.

ملخص

مع التطور المتسارع لإنترنت الأشياء، أصبح تأمين الاتصالات بين الأجهزة المتصلة تحديًا كبيرًا، لا سيما بسبب محدودية مواردها من حيث الطاقة والذاكرة والقدرة الحاسوبية. تقترح هذه الأطروحة بروتوكول مصادقة خفيف الوزن مخصصًا لأنظمة إنترنت الأشياء ذات الموارد المحدودة، مع اعتماد العدادات الذكية كدراسة حالة.

يعتمد البروتوكول على المصادقة المتبادلة بين العداد الذكي ومنصة المراقبة، باستخدام دوال التجزئة، والأرقام العشوائية، ورمز التحقق لمرة واحدة المرسل عبر تطبيق تيليجرام، بهدف ضمان سلامة وصحة البيانات المتبادلة وتعزيز الأمن السبيرياني.

أثبتت التجارب العملية، باستخدام لوحة ESP32 ومنصة مطورة بواسطة Visual Studio Code وقاعدة بيانات، فعالية البروتوكول في بيئة واقعية. كما أظهرت النتائج قدرته على مقاومة الهجمات الأمنية الرئيسية، مثل هجمات إعادة الإرسال وانتحال الهوية، مع الحفاظ على استهلاك منخفض للموارد.

وأخيرًا، أظهر التحليل المالي الأولي أن المشروع قابل للتطبيق من الناحية التقنية ومجدٍ اقتصاديًا، مما يجعله حلاً مناسبًا لتأمين أنظمة العدادات الذكية.

الكلمات المفتاحية: إنترنت الأشياء، المصادقة خفيفة الوزن، العداد الذكي، الأمن السبيرياني، رمز التحقق لمرة واحدة

Table des matières

Table des matières	i
Introduction générale	1
1 IoT et Cybersécurité dans l’IoT	3
1.1 Introduction :	3
1.2 Définition et concepts fondamentaux de l’IoT :	3
1.3 Historique de l’IoT :	4
1.4 Architecture des systèmes IoT(couche perception,couche réseau,couche ap- plication) :	5
1.5 Contraintes des objets IoT (énergie, calcul, mémoire) :	6
1.6 Les Domaines d’Application de l’IoT :	7
1.7 Avantages et inconvénients de l’IoT :	8
1.8 Les Défis de l’IoT :	8
1.8.1 Évolutivité :	9
1.8.2 Infrastructure réseau :	9
1.8.3 Hétérogénéité :	9
1.8.4 Interopérabilité :	10
1.8.5 Gestion de l’énergie :	10
1.8.6 cybersécurité et confidentialité :	10
1.9 La cybersécurité dans l’IoT :	10
1.9.1 Cybersécurité des données dans l’IoT :	10
1.9.2 cybersécurité des dispositifs IoT :	11
1.9.3 cybersécurité des communications IoT :	11

1.10	Objectifs de cybersécurité :	11
1.11	Menaces et attaques dans les environnements IoT :	12
1.12	Contraintes de cybersécurité dans l'IoT :	13
1.13	Solutions de cybersécurité IoT :	14
1.14	Conclusion :	15
2	Techniques d'authentification pour l'IoT	16
2.1	Introduction :	16
2.1.1	Importance de l'authentification dans l'IoT :	16
2.1.2	Objectif du chapitre :	16
2.2	Concepts généraux de l'authentification	16
2.2.1	Définition de l'authentification :	16
2.2.2	Différence : Authentification vs Autorisation	17
2.2.3	Types d'authentification :	17
2.3	Classification des techniques d'authentification IoT :	18
2.4	Problèmes et limites des solutions existantes	19
2.4.1	Consommation élevée :	19
2.4.2	Complexité :	19
2.4.3	Gestion des clés :	19
2.4.4	Vulnérabilités :	20
2.5	Définition du compteur intelligent :	20
2.6	Compteur intelligent comme dispositif IoT	20
2.7	Architecture typique :	20
2.8	Contraintes matérielles critiques :	21
2.9	Enjeux de cybersécurité :	22
2.10	Conclusion	22
3	Proposition et Analyse	24
3.1	Analyse du système Sonelgaz existant :	24
3.1.1	Architecture GSM / Modem / Plateforme HP :	24
3.1.2	Profil des compteurs MT/HT	25
3.1.3	Vulnérabilités identifiées : mots de passe faibles :	25
3.2	Contexte opérationnel de la télérelève :	26

3.3	Présentation de la carte ESP32 :	27
3.4	Exigences du protocole proposé :	29
3.4.1	Exigences fonctionnelles :	29
3.4.2	Exigences sécuritaires :	29
3.4.3	Exigences de performance (contraintes GSM) :	30
3.5	Conception du protocole	31
3.6	Analyse de cybersécurité :	33
3.6.1	Résistance aux attaques :	33
3.7	Comparaison avec l'existant :	35
3.8	Implémentation et simulation :	35
3.8.1	Environnement de développement :	36
3.8.2	Architecture expérimentale :	37
3.9	Étude de performance	37
3.9.1	Métriques d'évaluation	38
3.9.2	Temps d'exécution des opérations cryptographiques	38
3.9.3	Empreinte mémoire	40
3.9.4	Consommation énergétique	41
3.9.5	Complexité computationnelle	43
3.9.6	Taux de réussite et robustesse réseau	43
3.9.7	Comparaison synthétique des performances	44
3.9.8	Limites et contraintes identifiées	46
3.10	Conclusion	46
4	Guide de projet	48
4.1	Introduction	48
4.2	Premier axe : Présentation du projet	48
4.2.1	L'idée du projet :	48
4.2.2	Valeurs proposées :	49
4.2.3	Equipe de travail :	50
4.2.4	Objectifs du projet :	50
4.2.5	Calendrier de réalisation du projet :	51
4.3	Deuxième axe : Aspects innovants	51
4.3.1	Nature des innovations :	51

4.3.2	Domaines d'innovation :	52
4.4	Troisième axe : Analyse stratégique du marché :	53
4.4.1	Le segment du marché :	53
4.4.2	Mesure de l'intensité de la concurrence :	56
4.4.3	La stratégie marketing :	59
4.5	Quatrième axe : Plan de production et organisation	62
4.5.1	Processus d'obtention du service dans le système :	62
4.5.2	L'approvisionnement :	63
4.5.3	La main-d'œuvre :	64
4.5.4	Les principaux partenaires :	65
4.6	Cinquième axe : Plan financier	66
4.6.1	Les coûts et charges :	66
4.6.2	Chiffre d'affaires :	70
4.7	Les comptes de résultat attendus :	71
4.8	Sixième axe : Prototype expérimental	73
4.8.1	Environnements de développement :	73
4.8.2	Implémentation de la base de données	74
4.8.3	Interface de Programmation	75
4.9	Conclusion	83
Conclusion générale		85
Bibliographie		87
A Annexe A		91
B Annexe B		94
B.1	Modèle d'affaires :	94
B.1.1	Business Model Canvas :	94
B.1.2	BMC permet :	94
B.1.3	Le BMC de notre projet :	95

Introduction générale

L'IoT connaît aujourd'hui une expansion considérable et constitue l'une des technologies les plus prometteuses de la transformation numérique. Grâce à l'interconnexion de milliards d'objets intelligents capables de collecter, traiter et échanger des données, l'IoT est désormais présent dans de nombreux domaines tels que la santé, l'industrie, les villes intelligentes, l'agriculture et les réseaux électriques intelligents.

Cependant, cette évolution s'accompagne de nombreux défis, notamment en matière de cybersécurité. Les objets connectés disposent généralement de ressources limitées en termes de puissance de calcul, de mémoire et d'énergie, ce qui rend difficile l'utilisation des mécanismes de sécurité traditionnels. Parmi les services de sécurité indispensables, l'authentification occupe une place essentielle puisqu'elle permet de vérifier l'identité des entités communicantes avant tout échange de données. Une authentification insuffisamment sécurisée peut exposer les systèmes IoT à diverses attaques, telles que l'usurpation d'identité, l'attaque par rejeu, l'interception des communications ou encore les attaques de type MITM.

Dans ce contexte, il devient nécessaire de développer des protocoles d'authentification à la fois légers, efficaces et adaptés aux contraintes des objets connectés. L'objectif est d'assurer un niveau de cybersécurité satisfaisant tout en limitant la consommation des ressources matérielles des dispositifs IoT.

Le présent mémoire s'inscrit dans cette problématique et propose un protocole d'authentification léger destiné aux systèmes IoT contraints en ressources. Afin de rapprocher cette étude d'un contexte industriel réel, nous avons pris comme cas d'application le système de télérelève des compteurs intelligents utilisé dans les réseaux électriques. Le protocole

proposé repose sur un mécanisme d'authentification mutuelle utilisant des fonctions de hachage, des nonces, un code OTP transmis via Telegram ainsi qu'un échange sécurisé entre le compteur intelligent, la plateforme de supervision et le service de vérification.

Une implémentation expérimentale basée sur une carte ESP32 a ensuite été réalisée afin de valider le fonctionnement du protocole dans un environnement représentatif. Une analyse de sécurité a également permis d'évaluer sa résistance face aux principales attaques visant les systèmes IoT, notamment les attaques par rejeu, l'usurpation d'identité, l'interception des données et les attaques de type MITM. Enfin, une étude technico-économique a été menée afin d'évaluer la faisabilité du projet et son potentiel de valorisation.

Ce mémoire est organisé en quatre chapitres :

- **Le premier chapitre** présente les concepts fondamentaux de l'IoT, son architecture, ses contraintes ainsi que les principaux enjeux liés à la cybersécurité.
- **Le deuxième chapitre** est consacré aux techniques d'authentification dans les environnements IoT, aux solutions existantes ainsi qu'à leurs limites face aux objets contraints.
- **Le troisième chapitre** décrit le protocole proposé, son fonctionnement, son implémentation expérimentale ainsi que son analyse de sécurité.
- **Le quatrième chapitre** présente le guide de projet, incluant l'étude stratégique, le modèle économique, le plan financier et la réalisation du prototype expérimental.

À travers ce travail, nous cherchons à proposer une solution d'authentification simple, légère et adaptée aux objets connectés contraints, tout en démontrant sa faisabilité technique et son intérêt dans le domaine des infrastructures IoT sécurisées.

IoT et Cybersécurité dans l'IoT

1.1 Introduction :

IoT désigne l'ensemble des dispositifs connectés capables de collecter et d'échanger des données via Internet, avec plus de 15 milliards d'unités en circulation en 2025. Grâce à son développement rapide, l'IoT transforme des domaines comme la santé (surveillance à distance), l'industrie (maintenance prédictive) et les réseaux intelligents (gestion énergétique). Cependant, cette connectivité massive expose à des risques majeurs : les appareils IoT, limités en ressources, sont vulnérables aux attaques comme les botnets Mirai ou les interceptions de données. Il est donc crucial d'adopter des mécanismes adaptés, tels que des protocoles légers comme MQTT avec authentification forte, pour sécuriser les données et les communications [1].

1.2 Définition et concepts fondamentaux de l'IoT :

L'IoT a été introduite en 1999 au sein du Massachusetts Institute of Technology par Kevin Ashton, considéré comme l'un des précurseurs de ce concept. IoT fait référence à un réseau global composé d'objets physiques connectés à Internet, tels que des capteurs et des dispositifs intelligents, capables de communiquer entre eux. Ces objets collectent des données issues de leur environnement et les transmettent pour qu'elles soient analysées et exploitées par différents acteurs, notamment les entreprises, les institutions publiques, les villes intelligentes, les établissements de santé ainsi que les particuliers. Le développement

de l'IoT repose principalement sur les progrès réalisés dans les technologies électroniques et de communication. En effet, l'apparition de composants tels que les capteurs, les actionneurs, les cartes électroniques programmables et les réseaux sans fil a permis de transformer des objets ordinaires en objets connectés intelligents. Ces derniers peuvent désormais capter des informations, les traiter ou les transmettre à distance via des réseaux, facilitant ainsi leur intégration dans des systèmes intelligents [2].

1.3 Historique de l'IoT :

L'évolution de l'IoT s'est faite progressivement à travers plusieurs étapes marquantes, liées aux avancées technologiques en électronique et en réseaux.

- **1990 : Premières expérimentations :** Cette période marque l'apparition des premiers objets connectés expérimentaux. Il s'agissait principalement d'appareils du quotidien tels que des grille-pain ou des machines à café, capables d'être contrôlés ou supervisés à distance. Ces premières tentatives restent limitées mais posent les bases du concept d'objets communicants [1].
- **2000 : Début des objets connectés grand public :** Au début des années 2000, les premières applications concrètes d'objets connectés apparaissent. Des dispositifs capables de se connecter à Internet sont développés pour fournir des informations de manière automatique. Un exemple notable est Ambient Orb (2002), qui permettait de visualiser des données en temps réel. Par ailleurs, LG figure parmi les premiers industriels à proposer des appareils électroménagers connectés à Internet [1].
- **2008 : Standardisation et intégration IP :** En 2008, plusieurs grandes entreprises telles que Cisco, Intel, SAP et Sun Microsystems ont créé l'alliance IPSO. L'objectif était de promouvoir l'utilisation du protocole IP dans les dispositifs à faible consommation d'énergie.

Dans ce contexte, le groupe de travail 6LoWPAN , initié par Internet Engineering Task Force, a permis d'adapter le protocole IPv6 aux réseaux contraints basés sur la norme IEEE 802.15.4. Cela constitue une avancée majeure pour l'intégration des objets connectés dans l'Internet global [1].

- **2011 : Adoption d'IPv6 :** L'introduction du protocole IPv6 a permis de lever les limitations liées à l'épuisement des adresses IPv4. Grâce à son espace d'adressage

étendu, IPv6 offre la possibilité d'attribuer une adresse unique à chaque objet connecté, facilitant ainsi leur identification et leur communication à grande échelle [1].

- **2012 – aujourd'hui : Croissance massive de l'IoT** : À la fin de l'année 2012, on estimait à environ 8,7 milliards le nombre d'objets connectés dans le monde. Selon les études de BI Intelligence, ce nombre a connu une croissance rapide, atteignant plusieurs dizaines de milliards d'objets, avec un taux de croissance annuel important. Cette expansion est portée par le développement des technologies sans fil, du cloud computing et de l'intelligence artificielle [3].

1.4 Architecture des systèmes IoT (couche perception, couche réseau, couche application) :

Bien qu'il existe plusieurs modèles architecturaux pour l'IoT, la plupart reposent sur une organisation en couches permettant de structurer les fonctionnalités d'un système IoT de bout en bout. Cette approche facilite la conception, le déploiement et la gestion des systèmes en séparant les responsabilités selon des niveaux fonctionnels bien définis.

1. Couche de perception :

La couche de perception constitue le niveau le plus bas de l'architecture IoT. Elle assure la collecte des données à partir de l'environnement à l'aide de capteurs, actionneurs et technologies comme la RFID, permettant l'identification unique des objets via des codes tels que l'EPC.

2. Couche réseau :

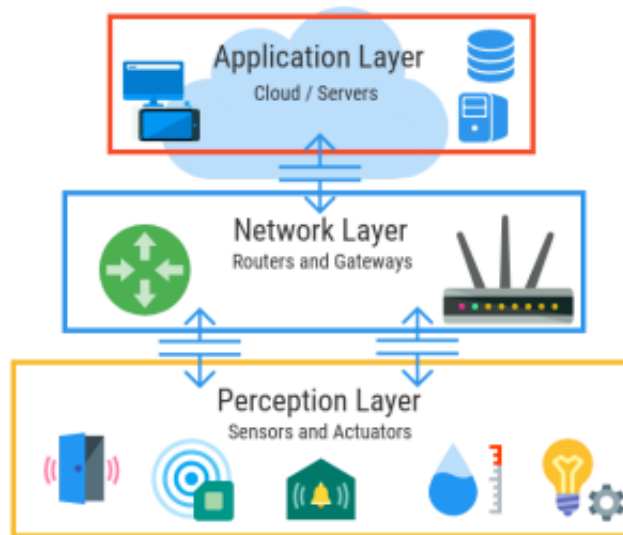
La couche réseau est responsable de la transmission des données vers les systèmes de traitement, en utilisant des technologies de communication filaires ou sans fil telles que Wi-Fi, Bluetooth, ZigBee, ou encore les réseaux cellulaires. Elle garantit un acheminement fiable des informations entre les objets connectés et les infrastructures distantes (serveurs, cloud).

3. Couche application :

La couche application représente le niveau supérieur de l'architecture IoT. Elle est chargée de l'analyse, du traitement des données et de la prise de décision. Les

informations reçues sont exploitées pour fournir des services intelligents adaptés aux besoins des utilisateurs.

Cette couche s'appuie sur des technologies avancées telles que le cloud computing et l'intelligence artificielle afin de transformer les données brutes en informations exploitables. Elle permet ainsi de réaliser des actions de contrôle et d'automatisation, en répondant à des questions comme : quoi faire, quand agir et comment optimiser le système. Les applications peuvent concerner divers domaines comme la domotique, la santé, l'industrie ou les villes intelligentes [4].



(a)

FIGURE 1.1 – Architecture du système IoT

1.5 Contraintes des objets IoT (énergie, calcul, mémoire) :

Les objets IoT sont caractérisés par des ressources limitées, notamment en termes d'énergie, de capacité de calcul et de mémoire. Ces contraintes influencent directement leur fonctionnement et imposent des choix spécifiques lors de la conception des systèmes, tant au niveau logiciel que des protocoles de communication réseau.

- **Contrainte d'énergie :**

La majorité des capteurs et microcontrôleurs utilisés dans les systèmes IoT sont alimentés par batterie ou par des sources d'énergie ambiante. Leur autonomie est donc limitée, variant généralement de quelques mois à quelques années selon les conditions d'utilisation et l'optimisation énergétique du système [5]. Les communications sans fil (Wi-Fi, Bluetooth, LoRa, etc.) sont énergivores, ce qui impose de limiter les transmissions, d'utiliser des modes veille et d'optimiser les données [6].

- **Contraintes de calcul :**

Les dispositifs IoT intègrent des microcontrôleurs 8, 16 ou 32 bits, dont la capacité de calcul reste largement inférieure à celle d'un smartphone, avec un écart pouvant atteindre un facteur de 10 à 150. Ces ressources limitées restreignent l'utilisation de bibliothèques lourdes, de mécanismes cryptographiques complexes ou de traitements avancés ; une partie du calcul est donc déportée vers le cloud ou une passerelle [7].

- **Contraintes de mémoire (RAM et stockage) :**

Les dispositifs IoT disposent généralement de ressources mémoire limitées, allant de quelques kilo-octets à quelques centaines de kilo-octets de RAM.

Ces contraintes imposent un code léger (OS embarqué minimal, sans frameworks lourds), une gestion stricte de la mémoire, un transfert rapide des données vers une passerelle ou le cloud, et l'évitement de toute redondance inutile [8].

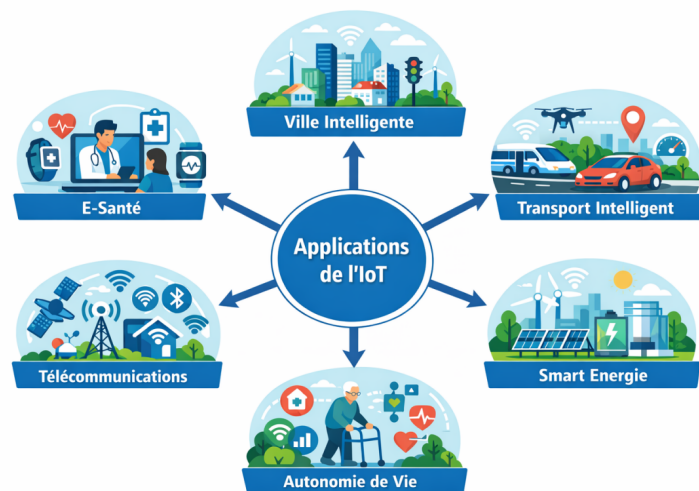
En conséquence, les architectures IoT s'appuient sur des réseaux de capteurs, des passerelles Edge et le cloud pour externaliser le calcul et le stockage, tandis que les objets terminaux se limitent à des tâches simples comme l'acquisition, le prétraitement et la transmission des données [5].

1.6 Les Domaines d'Application de l'IoT :

L'IoT offre de nombreuses applications dans divers secteurs :

- * **E-santé** : permet la surveillance à distance des patients, l'amélioration du suivi médical et l'accès aux données de santé en temps réel, facilitant ainsi le diagnostic et la prise en charge
- * **Ville intelligente** : utilise l'IoT, le cloud et l'analyse de données pour optimiser la gestion urbaine (transport, énergie, sécurité) et améliorer la qualité de vie des citoyens.

- * **Transport intelligent** : intègre des capteurs dans les véhicules pour surveiller des paramètres comme la vitesse, la pression ou la température, améliorant la cybersécurité et la gestion du trafic.
- * **Télécommunications** : combine plusieurs technologies (NFC, Bluetooth, ZigBee, Wi-Fi, etc.) pour offrir de nouveaux services connectés et améliorer la communication entre objets.
- * **Autonomie de vie (Assistance)** : aide les personnes âgées ou dépendantes grâce à des systèmes de surveillance (capteurs corporels, suivi des activités quotidiennes).
- * **Énergie intelligente** : Permet le suivi et l'optimisation de la consommation énergétique, réduisant les coûts tout en améliorant l'efficacité énergétique.



(a)

FIGURE 1.2 – Domaines d'Application IoT

1.7 Avantages et inconvénients de l'IoT :

Le tableau suivant présente les principaux avantages et inconvénients de l'IoT :

1.8 Les Défis de l'IoT :

Dans le contexte de l'IoT, un grand nombre de dispositifs connectés génèrent d'importants volumes de données. Lorsqu'elles sont correctement exploitées, ces données constituent

Avantages	Inconvénients
Amélioration de la collecte de données	Problèmes de cybersécurité
Suivi des biens et des consommateurs	Complexité des systèmes
Optimisation et amélioration des services	Manque de flexibilité
Interaction avec l'environnement (capteurs/actionneurs)	Risques liés aux systèmes connectés
Innovation et nouveaux services	Dépendance à Internet

TABLE 1.1 – Tableau des avantages et des inconvénients
[3].

une ressource essentielle pour les applications intelligentes dites context-aware, capables d'adapter dynamiquement les services en fonction de l'environnement. Toutefois, plusieurs défis majeurs doivent être surmontés pour assurer le déploiement efficace et à grande échelle de l'IoT [3].

1.8.1 Évolutivité :

La croissance rapide du nombre d'objets connectés engendre des problématiques liées à la gestion de systèmes de grande taille, à l'interconnexion massive et à l'intégration de ressources hétérogènes. La représentation numérique du monde physique ajoute également un niveau de complexité supplémentaire.

1.8.2 Infrastructure réseau :

L'infrastructure Internet actuelle présente des limites en termes de gestion, de mobilité, de disponibilité et de passage à l'échelle, ce qui freine l'intégration optimale des objets connectés.

1.8.3 Hétérogénéité :

Les dispositifs IoT diffèrent en termes de capacités, de fonctionnalités et de conditions de fonctionnement. Cette diversité rend leur intégration difficile et augmente la complexité globale du système, notamment lorsqu'ils sont combinés en réseaux complexes.

1.8.4 Interopérabilité :

L'interaction entre différents acteurs (objets, utilisateurs, services) nécessite une communication transparente. Or, les différences de protocoles, de formats et de gestion compliquent cette interopérabilité.

1.8.5 Gestion de l'énergie :

L'alimentation énergétique constitue une contrainte critique dans les systèmes IoT. Il est donc nécessaire de concevoir des solutions optimisées en termes de consommation, tant au niveau du calcul, du stockage que de la transmission des données.

1.8.6 cybersécurité et confidentialité :

La cybersécurité de l'IoT doit être assurée à tous les niveaux. Elle inclut la protection contre les attaques, la sécurisation des échanges de données, la préservation de la vie privée des utilisateurs ainsi que la gestion des identités et de la confiance entre les entités du système.

1.9 La cybersécurité dans l'IoT :

Correspond à l'ensemble des mesures techniques, organisationnelles et opérationnelles mises en œuvre afin d'assurer la protection des dispositifs connectés, des données qu'ils produisent ainsi que des communications qu'ils établissent. Elle vise à prévenir les cybermenaces telles que les intrusions, l'usurpation d'identité ou les attaques par DDoS, en s'appuyant sur les principes fondamentaux de la triade CIA [9].

1.9.1 Cybersécurité des données dans l'IoT :

Elle consiste à assurer la protection des informations collectées et transmises par les capteurs contre toute fuite, altération ou interception non autorisée. Cette protection repose notamment sur l'utilisation de mécanismes cryptographiques tels que le chiffrement (par exemple AES-256) et les fonctions de hachage (comme SHA-256), garantissant ainsi la confidentialité et l'intégrité des données [10].

1.9.2 cybersécurité des dispositifs IoT :

Elle consiste à protéger les objets connectés grâce à des mécanismes intégrés dans le matériel et le logiciel. Cela inclut l'authentification sécurisée (comme les certificats), l'utilisation de composants de cybersécurité (TPM) et les mises à jour à distance (OTA). Ces solutions permettent d'éviter les attaques liées à des failles simples, comme les mots de passe par défaut [11].

1.9.3 cybersecurité des communications IoT :

Elle vise à protéger les échanges de données entre les objets connectés en utilisant des protocoles sécurisés comme TLS ou MQTT. Ces mécanismes garantissent la confidentialité et l'intégrité des informations lors de leur transmission sur différents réseaux (Wi-Fi, 5G, LoRa) [12].

1.10 Objectifs de cybersécurité :

Triade CIA ,ces trois piliers forment la base de toute stratégie de cybersécurité de l'information.

1. **Confidentialité** : Elle assure que seules les entités autorisées peuvent accéder aux informations sensibles, grâce à des mécanismes tels que le contrôle d'accès, le chiffrement et l'authentification multifactorielle [13].
2. **Intégrité** : Elle garantit que les données demeurent exactes, complètes et non modifiées, en s'appuyant sur des mécanismes tels que les fonctions de hachage ou les signatures numériques pour détecter toute altération [14].
3. **Disponibilité** : Elle garantit un accès continu et fiable aux informations pour les utilisateurs autorisés, grâce à des mécanismes tels que la redondance et les plans de reprise après sinistre [15].

Certains cadres, comme ISO 27001, intègrent deux notions supplémentaires.

1. **Authenticité** : Elle garantit la vérification de l'origine des données ainsi que l'identité des entités (utilisateurs ou dispositifs) impliquées [16].
2. **Non-répudiation** : Elle garantit qu'une entité ne peut nier avoir réalisé une action, grâce à des mécanismes de preuve tels que les signatures numériques [17].

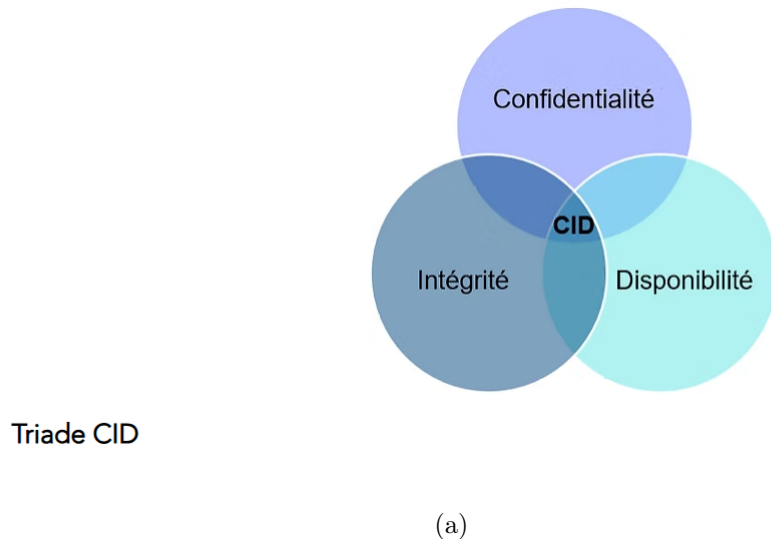


FIGURE 1.3 – Triade CIA

1.11 Menaces et attaques dans les environnements IoT :

L'IoT permet l'interconnexion de milliards de dispositifs dans la vie quotidienne, mais ces systèmes restent fortement exposés à diverses cyberattaques. Cette section présente les principales menaces et types d'attaques ciblant les environnements IoT, les attaques par rejeu, usurpation d'identité, MITM et interception [18].

- **Attaque par rejeu :**

Une attaque par rejeu consiste à intercepter un message valide, puis à le retransmettre ultérieurement de manière frauduleuse afin de tromper le système cible, sans nécessiter le déchiffrement du contenu. Dans le contexte de l'IoT, ce type d'attaque exploite les protocoles dépourvus de mécanismes de protection tels que les horodatages ou les valeurs uniques (nonce), permettant ainsi la réutilisation de commandes ou de messages légitimes [19].

- **Usurpation d'identité :**

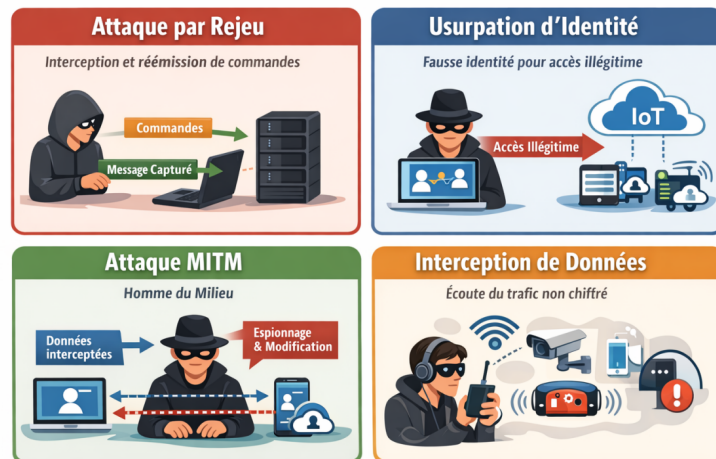
L'usurpation d'identité consiste pour un attaquant à se faire passer pour une entité légitime (utilisateur, dispositif ou service) afin d'accéder de manière frauduleuse à des ressources IoT ou à des données hébergées dans le cloud. Dans les environnements IoT, cette attaque peut viser les dispositifs connectés pour en prendre le contrôle ou accéder à des informations sensibles [20].

- **Attaque MITM :**

Cette attaque consiste à insérer un attaquant entre deux entités communicantes afin d'intercepter, modifier ou supprimer des messages à leur insu. Elle exploite généralement des protocoles de communication insuffisamment sécurisés. Dans les environnements IoT, cette vulnérabilité est accentuée par l'utilisation de réseaux Wi-Fi non sécurisés ou de protocoles tels que Diffie-Hellman sans mécanisme d'authentification [21].

- **Interception :**

L'interception consiste à capter les données échangées sur un réseau, généralement via des techniques telles que le sniffing ou l'utilisation d'outils comme les IMSI catchers, afin d'analyser le trafic sans en modifier le contenu. Dans les environnements IoT, ce type d'attaque permet d'accéder à des informations sensibles lorsque les communications ne sont pas chiffrées [22].



(a)

FIGURE 1.4 – Menaces et attaques

1.12 Contraintes de cybersécurité dans l'IoT :

Les contraintes de cybersécurité dans l'IoT résultent des limitations matérielles (faible CPU/mémoire), des réseaux hétérogènes vulnérables et de l'absence de mises à jour, rendant difficile l'application de la triade CIA face aux cybermenaces.

- **Contraintes matérielles** : les objets IoT ont peu de mémoire et de puissance. Cela rend difficile l'utilisation de solutions de cybersécurité complexes, tout en demandant un fonctionnement rapide [23].
- **Contraintes réseau** : les objets IoT utilisent différents types de réseaux (Wi-Fi, LoRa, etc.), souvent peu sécurisés. Cela les expose à des attaques comme l'interception des données, MITM ou les attaques DDoS [14].
- **Contraintes de mise à jour** : Beaucoup d'objets IoT ne reçoivent pas de mises à jour automatiques. Cela laisse des failles de cybersécurité non corrigées, surtout lorsque les fabricants arrêtent le support [23].
- **Contraintes d'authentification** : l'utilisation de mots de passe par défaut et de contrôles d'accès faibles facilite l'usurpation d'identité et les accès non autorisés [24].
- **Contraintes organisationnelles** : La diversité des acteurs et le manque de normes communes font que la cybersécurité est souvent négligée au profit du coût dès la conception [25].

1.13 Solutions de cybersécurité IoT :

Les solutions spécifiques pour l'IoT ciblent les ressources limitées via la cryptographie légère, des protocoles d'authentification efficaces et une gestion dynamique des clés.

1. Cryptographie légère :

- Fonctions de hachage : ASCON-Hash, SHA-3 lightweight pour l'intégrité avec une faible consommation [26].
- XOR : Opérations simples pour le masquage rapide dans des capteurs contraints.
- Chiffrement lightweight : ASCON-128, PRESENT/AES-Speck pour 128 bits de sécurité sur microcontrôleurs [27].

2. Protocoles d'authentification :

- Challenge-response : Échange non réutilisable évitant l'attaque par rejeu, adapté aux dispositifs légers [28].
- Hash-based authentication : HB+ et Lamport sont des méthodes d'authentification légères pour IoT utilisant des fonctions de hachage, adaptées aux appareils à faible puissance sans certificats complexes [29].

3. Gestion des clés :

- Clés dynamiques : Génération session par session via ECDH lightweight [30].
- Renouvellement des clés : OTA automatisé avec rotation périodique pour limiter l'exposition [31].

1.14 Conclusion :

En conclusion, l'IoT représente une avancée majeure en interconnectant des milliards de dispositifs intelligents dans des domaines variés comme la santé ou l'industrie. Néanmoins, cette expansion génère des défis sécuritaires critiques, dus aux ressources limitées des objets et à leur exposition aux cybermenaces comme les botnets.

Il est impératif d'adopter des solutions adaptées, notamment des protocoles d'authentification légers et une architecture zero-trust, pour assurer la confidentialité, l'intégrité et la disponibilité des données dans les ecosystems IoT.

Techniques d'authentification pour l'IoT

2.1 Introduction :

L'authentification représente un élément essentiel de la cybersécurité dans l'IoT, permettant de vérifier l'identité des nombreux appareils connectés afin de prévenir les accès non autorisés et de protéger les données sensibles [32].

2.1.1 Importance de l'authentification dans l'IoT :

L'authentification permet d'établir une relation de confiance entre les objets IoT, les passerelles et les systèmes centraux, en empêchant les attaques d'usurpation d'identité pouvant perturber le bon fonctionnement des réseaux [33].

2.1.2 Objectif du chapitre :

Ce chapitre présente les techniques d'authentification adaptées (certificats X.509, TPM, HB+/Lamport lightweight) pour sécuriser les communications IoT, avec un focus sur les applications compteur intelligent nécessitant des protocoles ultra-légers.

2.2 Concepts généraux de l'authentification

2.2.1 Définition de l'authentification :

L'authentification est un mécanisme de cybersécurité qui permet à un système informatique de vérifier l'identité d'une entité (utilisateur, appareil IoT ou service) en contrôlant

ses identifiants, tels que les certificats, les clés ou les tokens, avant de lui autoriser l'accès aux ressources [34].

2.2.2 Différence : Authentification vs Autorisation

Critère	Authentification	Autorisation
Question	Qui êtes-vous ?	Que pouvez-vous faire ?
Objectif	Vérifier identité	Définir privilèges d'accès
Séquence	Première étape	Après authentification réussie
Exemple IoT	Smart meter valide son identité	Accès aux données de consommation Fortinet+1

TABLE 2.1 – Différence
[35]

2.2.3 Types d'authentification :

1. Authentification unilatérale :

Il s'agit d'un mécanisme dans lequel une seule entité est vérifiée lors de la communication. Dans ce cas, seul le client (smart meter) prouve son identité au serveur (gateway) [36].

2. Authentification mutuelle :

Il s'agit d'un mécanisme dans lequel les deux entités en communication vérifient leur identité. Par exemple, avec mTLS, le client et le serveur s'authentifient mutuellement en échangeant des certificats numériques [37].

Critère	Unilatérale	Mutuelle
Sens	Client $\rightarrow$ Serveur	Client $\leftrightarrow$ Serveur
Protocole	TLS standard	mTLS, Challenge-Response
IoT	Connexion basique	Smart meters critiques

TABLE 2.2 – Types d'authentification
[38]

2.3 Classification des techniques d'authentification IoT :

1. Authentification basée sur mot de passe :

* **Authentification par mot de passe** : elle repose sur l'utilisation d'un identifiant et d'un mot de passe partagés entre le dispositif IoT et le serveur. Ces informations sont stockées de manière sécurisée (hachées) côté serveur. Lors de la connexion, le dispositif envoie ses identifiants, qui sont ensuite vérifiés par comparaison pour autoriser l'accès [39].

* **Limites**

- Mots de passe par défaut "admin/admin" (Mirai 2016)
- Force brute 10^6 tentatives/s
- Impossible MFA sur IoT contraint

2. Authentification basée sur certificats :

- X.509 : Certificats numériques avec chaîne de confiance pour l'identité forte.
- TLS : Protocole sécurisant les communications (handshake + chiffrement).
- Limites IoT : Coût computationnel élevé, mémoire flash limitée (4 MB ESP32).

3. Authentification par clé partagée :

- * Clé symétrique : secret commun (AES-128) pour chiffrement/authentification mutuelle.
- * Avantages : Léger, rapide.
- * Inconvénients : distribution sécurisée difficile, compromission = réseau entier vulnérable.

4. Authentification basée sur fonctions de hachage

- * Principe : Preuve connaissance secrète via hachage sans transmission directe.
- * SHA-256 : 256 bits, collision-resistant.
- * SHA-3 : Éponge Keccak, quantum-résistant.
- * IoT : Lamport signatures, Merkle trees pour smart meters [40].

5. Authentification Challenge-Response :

- * Principe : serveur envoie nonce (défi aléatoire), client répond $H(\text{nonce} + \text{clé})$.
- * Nonce : Valeur unique/session évitant attaques par replay.
- * Protection : Nonce périmé après usage [41].

6. **Protection : Nonce périmé après usage** : Il s'agit de protocoles conçus pour fonctionner sur des microcontrôleurs à ressources limitées (8 ou 32 bits), en utilisant des mécanismes simples et rapides adaptés aux dispositifs IoT.

Caractéristiques :

- * Faible coût computationnel
- * Faible consommation énergétique

Exemples :

- * HB+ :LPN
- * Lamport : Hash-based one-time signatures [42].

2.4 Problèmes et limites des solutions existantes

Les solutions traditionnelles d'authentification IoT échouent face aux contraintes matérielles des appareils.

2.4.1 Consommation élevée :

PKI/TLS RSA-2048 épuise les batteries IoT (10 ans requis pour le compteur intelligent) : ESP32 520KB SRAM $\rightarrow$ AES 50x plus économe [43].

2.4.2 Complexité :

Chaîne certificats + CRL/OCSP incompatible microcontrôleurs : Gestion CA centralisée requise [44].

2.4.3 Gestion des clés :

Distribution de 1M+ clés d'usine, rotation OTA impossible, compromission = réseau entier vulnérable [45].

2.4.4 Vulnérabilités :

Solution	Vulnérabilité	Source
Mot de passe	Mots par défaut	sentinelone
PKI	Certificats périmés	Fortinet
Symétrique	Distribution	Splashtop
TLS	Padding oracle	Fortinet

TABLE 2.3 – Vulnérabilités

2.5 Définition du compteur intelligent :

Le **compteur intelligent** : C'est un dispositif capable de mesurer de manière précise et en temps réel la consommation d'énergie (électricité, gaz ou eau). Il transmet ces données automatiquement, via des technologies de communication telles que les réseaux radio ou le courant porteur, vers un système central permettant leur analyse et leur exploitation [46].

2.6 Compteur intelligent comme dispositif IoT

Le compteur intelligent constitue comme IoT, car il :

- collecte des données en temps réel.
- communique avec une passerelle.
- transmet les informations vers le cloud [47].

Il permet également l'analyse des comportements de consommation énergétique.

2.7 Architecture typique :

Un système de compteur intelligent peut être composé de :

- Capteur (ex : PZEM004T).
- Microcontrôleur.
- Batterie longue durée (jusqu'à 10 ans).

- Passerelle.
- Cloud / serveur.



(a)

FIGURE 2.1 – compteur intelligent

2.8 Contraintes matérielles critiques :

Contrainte	Description	Impact sur la cybersécurité
Énergie	Consommation très faible	Impossible d'utiliser des algorithmes lourds (RSA, ECC)
Mémoire	Capacité limitée (ex : ESP32 4MB)	Difficulté d'utiliser des certificats X.509
Déploiement	Grand nombre d'unités (millions)	Gestion PKI complexe

TABLE 2.4 – Contraintes matérielles

[48].

2.9 Enjeux de cybersécurité :

Les compteurs intelligents manipulent des données sensibles, notamment :

- consommation énergétique.
- habitudes de vie des utilisateurs.

Ils sont également exposés à :

- réseaux non sécurisés.
- attaques réseau.

Par conséquent :

- une authentification sécurisée est indispensable.
- des mécanismes légers doivent être utilisés.
- Justification de l'authentification légère.

En raison des contraintes des compteurs intelligents :

- énergie limitée.
- mémoire limitée.
- déploiement massif.

Les solutions classiques (PKI, RSA, ECC) sont difficiles à implémenter.

Il devient donc nécessaire d'utiliser des protocoles d'authentification légère basés sur :

- fonctions de hachage.
- opérations simples [48].

2.10 Conclusion

Dans ce chapitre, nous avons étudié les différentes techniques d'authentification utilisées dans les systèmes IoT, en mettant en évidence leurs caractéristiques ainsi que leurs limites. Il apparaît que les solutions classiques, bien qu'efficaces, ne sont pas toujours adaptées aux contraintes des dispositifs IoT, notamment en termes de ressources limitées.

L'analyse du compteur intelligent en tant que dispositif IoT a permis de souligner les défis spécifiques liés à la cybersécurité, tels que la protection des données sensibles et la résistance aux attaques réseau. Ces contraintes rendent nécessaire l'utilisation de mécanismes d'authentification à la fois efficaces et légers.

Ainsi, le recours à des protocoles d'authentification légère constitue une approche adaptée pour répondre aux exigences des environnements contraints. Toutefois, les solutions existantes présentent encore certaines limites, ce qui justifie la nécessité de proposer une nouvelle approche.

Dans ce contexte, le chapitre suivant est consacré à la conception et à la présentation du protocole proposé, visant à améliorer la cybersécurité des communications des compteurs intelligents tout en respectant leurs contraintes.

Proposition et Analyse

3.1 Analyse du système Sonelgaz existant :

Dans le contexte de la gestion des compteurs intelligents, Sonelgaz utilise une infrastructure de télérelève et de supervision permettant la collecte à distance des données de consommation énergétique. Cette architecture s'appuie sur différents moyens de communication, tels que le réseau GSM, des modems de transmission ainsi qu'une plateforme centrale dédiée au traitement et à la supervision des données.

L'analyse de ce système permet de mettre en évidence ses atouts en matière de supervision, mais aussi ses limites sur le plan de la cybersécurité, ce qui justifie l'étude d'une solution d'authentification plus légère et mieux adaptée aux contraintes des compteurs.

3.1.1 Architecture GSM / Modem / Plateforme HP :

L'architecture de communication d'un système de télérelève basé sur le réseau GSM s'organise autour de trois éléments principaux : le compteur intelligent, le modem de communication et la plateforme centrale de supervision.

Le compteur intelligent assure la collecte des données de consommation, tandis que le modem GSM se charge de leur transmission à travers le réseau mobile de l'opérateur. Les informations sont ensuite acheminées vers une plateforme centrale où elles sont stockées, analysées et exploitées pour des opérations telles que la facturation, la supervision ou le suivi énergétique.

Cette architecture offre plusieurs avantages, notamment la possibilité d'effectuer une sur-

veillance à distance des installations, particulièrement dans les environnements industriels ou les zones difficiles d'accès. Cependant, son efficacité dépend fortement de la disponibilité du réseau de communication ainsi que de la fiabilité des mécanismes de sécurité et d'authentification mis en œuvre entre les différents équipements et la plateforme centrale.

3.1.2 Profil des compteurs MT/HT

Les compteurs MT/HT sont généralement déployés dans les environnements industriels et les infrastructures nécessitant une consommation énergétique importante.

Le catalogue officiel de Sonelgaz mentionne l'utilisation des compteurs industriels MT/HT, confirmant leur rôle essentiel dans les systèmes de télérelève et de gestion énergétique des installations à forte consommation [49].

Contrairement aux compteurs résidentiels, les compteurs MT/HT gèrent des charges énergétiques importantes et nécessitent des mécanismes de communication fiables afin d'assurer l'exactitude des mesures et la continuité des opérations de supervision et de facturation [50].

Dans ce contexte, une altération ou une manipulation des données de mesure peut affecter directement la précision de la facturation, la supervision énergétique et l'intégrité globale du système de télérelève.

3.1.3 Vulnérabilités identifiées : mots de passe faibles :

Parmi les faiblesses de cybersécurité fréquemment observées dans les systèmes de télérelève figure l'utilisation d'identifiants par défaut ou de mots de passe peu robustes, augmentant le risque d'accès illégitime aux dispositifs et aux plateformes de supervision.

Des recherches sur la cybersécurité des systèmes des compteurs intelligents montrent qu'un attaquant peut tirer parti de mécanismes d'authentification insuffisants pour compromettre la confidentialité, l'intégrité ou la disponibilité du système .

Cela montre la nécessité d'adopter un mécanisme d'authentification plus robuste, tout en

restant compatible avec les contraintes matérielles des compteurs intelligents .

3.2 Contexte opérationnel de la télérelève :

La campagne de télérelève est généralement exécutée de manière périodique. Dans le scénario considéré, la relève est déclenchée automatiquement le premier jour de chaque mois à 00h00 afin de récupérer la consommation cumulée du mois précédent. Par exemple, le 01 juin à 00h00, le système collecte la consommation totale enregistrée durant le mois de mai.

L'infrastructure centrale est composée de plusieurs équipements de communication permettant de gérer simultanément un grand nombre de compteurs. La plateforme dispose notamment de 18 modems GSM/GPRS et de deux serveurs de communication chargés d'assurer les échanges avec les compteurs déployés sur le terrain.

Afin d'optimiser la charge de travail et d'améliorer la disponibilité du système, le compteur n'est pas associé de manière permanente à un modem particulier. Lors d'une opération de télérelève, n'importe quel modem disponible peut être utilisé pour établir la communication avec le compteur. Cette architecture offre une meilleure tolérance aux pannes et garantit la continuité du service en cas d'indisponibilité d'un modem.

La gestion des demandes de télérelève repose sur un mécanisme de file d'attente. Lorsqu'une communication échoue, le système effectue automatiquement jusqu'à trois tentatives de connexion avant de déclarer un échec de relève. Cette stratégie permet d'augmenter le taux de réussite des collectes tout en limitant les surcharges du réseau.

Chaque compteur est associé à un PDL, qui constitue l'identifiant fonctionnel de l'installation électrique. Le PDL permet de rattacher les informations de consommation à un client spécifique et de conserver l'historique des télérelèves dans la base de données de la plateforme. L'ensemble des mesures collectées est ainsi archivé afin de permettre le suivi de la consommation, l'établissement de la facturation et l'analyse des performances énergétiques.

Au-delà de la collecte des consommations, le système assure également la supervision des

équipements grâce à la gestion des alarmes techniques. Ces alarmes permettent de détecter différents événements susceptibles d'affecter le fonctionnement normal du compteur ou du système de communication. Parmi les alarmes les plus courantes figurent l'ouverture du capot du compteur, les anomalies de tension, les défauts de communication ainsi que les défaillances matérielles telles que la détérioration ou la brûlure d'un modem.

L'analyse de ces alarmes permet aux opérateurs d'intervenir rapidement en cas d'incident et contribue à améliorer la fiabilité globale du système de télérelève.

Malgré les mécanismes de supervision existants, plusieurs vulnérabilités demeurent possibles au niveau de l'authentification des équipements. Dans certains scénarios, les compteurs peuvent être configurés avec des mots de passe communs ou par défaut. Par exemple, l'utilisation d'un mot de passe identique pour l'ensemble des compteurs augmente considérablement les risques d'usurpation d'identité et d'accès non autorisé au système.

3.3 Présentation de la carte ESP32 :

Dans le cadre de ce projet, la carte ESP32 a été choisie pour représenter le compteur intelligent. L'ESP32 est un microcontrôleur développé par Espressif Systems, intégrant des fonctionnalités de communication sans fil Wi-Fi et Bluetooth, ce qui en fait une solution particulièrement adaptée aux applications de IoT.

Contraintes de l'ESP32 :

- **Énergie :**
 - * Fonctionnement sur batterie possible.
 - * Nécessité de réduire les transmissions radio et les calculs inutiles.
- **Calcul :**
 - * Microcontrôleur double cœur jusqu'à 240 MHz.
 - * Ressources limitées pour les algorithmes cryptographiques complexes.
- **Mémoire :**
 - * Environ 520 Ko de RAM.

* Capacité limitée pour le stockage des historiques et des journaux.

Dans l'architecture proposée, l'ESP32 joue le rôle de compteur intelligent en collectant les données de consommation électrique, en exécutant les mécanismes de sécurité du protocole LHAM et en transmettant les informations vers la plateforme de supervision à travers une connexion Wi-Fi.

Le choix de l'ESP32 repose sur plusieurs avantages, notamment son faible coût, sa faible consommation énergétique, ses capacités de calcul adaptées aux applications IoT et sa compatibilité avec les algorithmes cryptographiques utilisés dans ce projet, tels que HMAC-SHA256 et la génération de clés de session.

Malgré ses performances, l'ESP32 reste soumis à certaines contraintes inhérentes aux objets connectés, notamment une mémoire limitée, une puissance de calcul inférieure à celle d'un ordinateur classique et des ressources énergétiques qui doivent être optimisées. Ces contraintes justifient l'utilisation d'un protocole de sécurité léger capable de garantir l'authenticité et l'intégrité des échanges tout en préservant les ressources du dispositif.

Ainsi, l'ESP32 constitue une plateforme expérimentale pertinente pour la validation du protocole de télérelève sécurisée proposé dans ce mémoire.

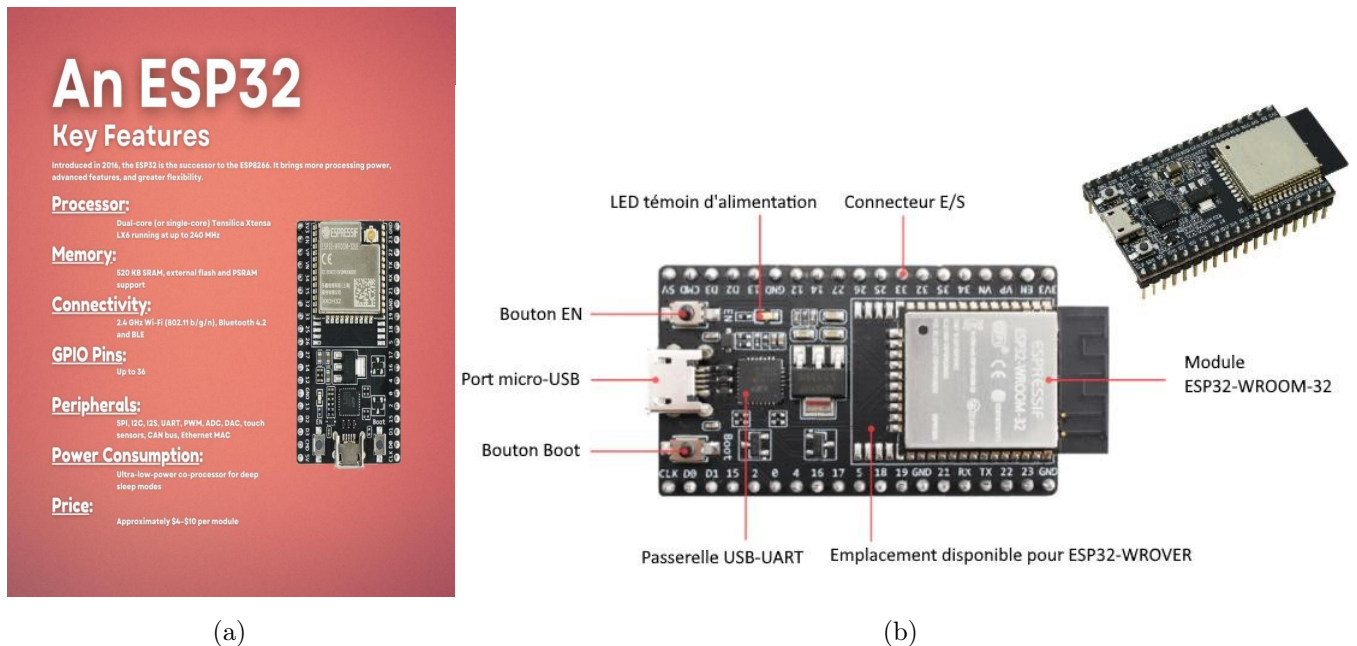


FIGURE 3.1 – Carte ESP32

3.4 Exigences du protocole proposé :

Afin de garantir une authentification fiable et sécurisée dans un environnement IoT contraint, le protocole proposé doit satisfaire un ensemble d'exigences fonctionnelles, sécuritaires et de performance. Ces exigences tiennent compte des contraintes des compteurs intelligents utilisant des modules GSM ainsi que des ressources limitées des dispositifs IoT.

3.4.1 Exigences fonctionnelles :

Le protocole proposé doit assurer les fonctionnalités nécessaires au bon fonctionnement du système de télérelève intelligent.

1. **Authentification mutuelle** : le compteur intelligent et la plateforme centrale doivent être capables de vérifier mutuellement leurs identités avant tout échange de données. Cette authentification bidirectionnelle permet d'éviter qu'un équipement malveillant ou un serveur non autorisé puisse participer au système.
2. **Identification unique du compteur intelligent** : chaque compteur intelligent doit disposer d'un identifiant unique lui permettant d'être reconnu par la plateforme centrale. Cet identifiant facilite la gestion des équipements et le suivi des opérations.
3. **Transmission sécurisée des données** : le protocole doit permettre le transfert des données de consommation énergétique entre le compteur intelligent et la plateforme tout en préservant leur intégrité et leur confidentialité.
4. **Gestion des sessions d'authentification** : chaque session doit être indépendante des précédentes afin d'éviter toute réutilisation frauduleuse des informations échangées.
5. **Compatibilité avec l'infrastructure GSM existante** : le protocole doit pouvoir fonctionner sur les réseaux GSM déjà utilisés dans les systèmes de télérelève sans nécessiter de modification importante de l'infrastructure existante.

3.4.2 Exigences sécuritaires :

La cybersécurité constitue un élément fondamental du protocole proposé.

1. **Confidentialité des informations** : Les données échangées ne doivent pas être accessibles à des entités non autorisées lors de leur transmission sur le réseau GSM.

2. **Intégrité des messages** : Toute modification des messages durant leur transmission doit être détectée afin d'empêcher l'altération des données de consommation ou des informations d'authentification.
3. **Protection contre les attaques par replay** : Le protocole doit empêcher un attaquant de réutiliser des messages précédemment capturés afin d'obtenir un accès illégitime au système. Cette protection est assurée par l'utilisation de nonces générés aléatoirement pour chaque session.
4. **Protection contre l'usurpation d'identité** : Un attaquant ne doit pas pouvoir se faire passer pour un compteur intelligent légitime ou pour la plateforme centrale.
5. **Résistance aux attaques de type MITM** : Le protocole doit être capable de détecter toute tentative d'interception ou de modification des échanges entre le compteur intelligent et la plateforme.
6. **Traçabilité des opérations** : Toutes les tentatives d'authentification doivent être enregistrées afin de faciliter l'audit de sécurité et l'analyse des incidents.

3.4.3 Exigences de performance (contraintes GSM) :

Le protocole doit être adapté aux limitations des dispositifs IoT et aux caractéristiques des réseaux GSM.

1. **Faible consommation énergétique** : Les opérations cryptographiques utilisées doivent être légères afin de préserver l'autonomie énergétique des compteurs intelligents alimentés par batterie.
2. **Faible occupation mémoire** : Le protocole doit nécessiter un espace mémoire réduit afin de rester compatible avec les ressources limitées de l'ESP32 et des équipements similaires.
3. **Faible complexité computationnelle** : Le protocole doit privilégier des opérations légères telles que les fonctions de hachage, les opérations XOR et la génération de nonces, plutôt que des mécanismes cryptographiques lourds basés sur une infrastructure à clés publiques.
4. **Adaptation aux variations du réseau GSM** : Le protocole doit continuer à fonctionner correctement malgré les fluctuations du signal GSM, les pertes de paquets ou les délais de transmission variables.

3.5 Conception du protocole

1. Présentation du scénario du protocole proposé

Le protocole proposé repose sur trois entités principales qui collaborent afin d'assurer une authentification sécurisée avant la transmission des données de télérelève.

- **Le compteur intelligent (ESP32)** : dispositif IoT chargé de mesurer la consommation électrique, de générer les informations de télérelève et de contrôler les différentes étapes d'authentification avant toute transmission des données.
- **La plateforme de supervision (Flask)** : serveur central responsable de l'envoi des demandes de télérelève, de la gestion de l'authentification, de la réception des données ainsi que de leur stockage dans la base de données.
- **Telegram** : service de messagerie utilisé comme canal sécurisé pour transmettre un mot de passe à usage unique (OTP) à l'utilisateur autorisé, constituant ainsi un second facteur d'authentification.

L'objectif principal de ce protocole est de garantir que seules les plateformes autorisées puissent accéder aux données du compteur intelligent, tout en protégeant le système contre les attaques d'usurpation d'identité, de rejeu et les accès non autorisés.

2. Phases du protocole proposé

Le protocole se déroule selon quatre phases successives.

- **Phase 1 : Initialisation de la communication**

La plateforme de supervision identifie le compteur intelligent concerné puis lui envoie une requête de télérelève. Cette requête déclenche le processus d'authentification entre les deux entités.

- **Phase 2 : Authentification par challenge-réponse**

À la réception de la requête, le compteur intelligent génère un nombre aléatoire unique (*nonce*) qu'il transmet à la plateforme. À partir de ce nonce et de la clé secrète partagée entre les deux entités, la plateforme calcule une réponse d'authentification qu'elle renvoie au compteur. Celui-ci vérifie la validité de cette réponse avant de poursuivre la communication. Cette phase assure une authentification mutuelle et protège le protocole contre les attaques par rejeu.

- **Phase 3 : Vérification du code OTP via Telegram**

Une fois l'authentification challenge-réponse validée, le compteur intelligent génère un code OTP à usage unique. Ce code est envoyé à l'utilisateur autorisé via Telegram. Le compteur informe ensuite la plateforme qu'il est en attente de la saisie du code en lui transmettant le message `WAITING_CODE`.

L'utilisateur récupère le code OTP reçu sur Telegram et le saisit dans l'interface de la plateforme de supervision. Cette dernière transmet alors le code au compteur intelligent qui vérifie sa validité. Cette étape constitue un second facteur d'authentification, renforçant considérablement la sécurité du protocole.

- **Phase 4 : Transmission des données de télérelève**

Si le code OTP est validé, le compteur intelligent autorise la transmission des données de télérelève vers la plateforme de supervision. Les informations transmises comprennent notamment :

- l'index de consommation électrique ;
- les mesures de télérelève demandées (tension, courant, puissance, énergie, etc.) ;
- les éventuels indicateurs ou informations complémentaires associés.

À la réception de ces données, la plateforme les stocke dans la base de données avant de les afficher sur le tableau de bord de supervision. Une fois cette opération terminée, le compteur intelligent revient à son état d'attente jusqu'à la prochaine demande de télérelève.

***Objectifs de sécurité atteints par le protocole :**

Le protocole proposé permet :

- l'authentification du compteur intelligent ;
- l'authentification de la plateforme ;
- la protection contre les attaques par rejeu grâce au nonce ;
- la protection contre l'usurpation d'identité ;
- la validation en deux étapes grâce à Telegram OTP ;
- la traçabilité des opérations d'authentification ;
- la sécurisation de l'accès aux données de consommation.

Cette architecture est particulièrement adaptée aux systèmes de télérelève GSM utilisés dans les infrastructures de comptage intelligent de type Sonelgaz.

3.6 Analyse de cybersécurité :

3.6.1 Résistance aux attaques :

1. **Résistance aux attaques par rejeu :** Les attaques par rejeu consistent à intercepter un message d'authentification valide, puis à le retransmettre ultérieurement afin d'obtenir un accès non autorisé au système. Dans le protocole proposé, chaque session d'authentification débute par la génération d'un *nonce* aléatoire par le compteur intelligent. Ce *nonce*, unique pour chaque session, est intégré au calcul de la réponse

d'authentification en combinaison avec la clé secrète partagée. Ainsi, même si un attaquant parvient à intercepter un message d'authentification valide, il ne pourra pas le réutiliser lors d'une nouvelle session, puisque le *nonce* associé sera différent et que la réponse calculée ne sera plus valide. Toute tentative de réutilisation d'un ancien message est donc détectée et rejetée par le serveur. Par conséquent, le protocole garantit une protection efficace contre les attaques par rejeu, tout en préservant sa légèreté et son faible coût de calcul, caractéristiques essentielles pour les objets IoT à ressources limitées.

2. **Résistance à l'usurpation d'identité :** L'usurpation d'identité vise à faire passer un attaquant pour un compteur intelligent légitime ou pour la plateforme centrale. Le protocole utilise un mécanisme d'authentification basé sur :

- l'identifiant du compteur intelligent ;
- un secret partagé ;
- nonce.

Un attaquant ne possédant pas les informations secrètes nécessaires est incapable de générer une réponse d'authentification valide.

De plus, la validation OTP transmise via Telegram constitue un second niveau de vérification empêchant l'accès frauduleux au système.

3. **Résistance aux attaques MITM :** Dans une attaque de type MITM, l'attaquant

tente d'intercepter et de modifier les messages échangés entre le compteur et la plateforme.

Le protocole réduit ce risque grâce à :

- la vérification du nonce ;
- la validation de la réponse d'authentification ;
- la vérification du code OTP.

Toute modification des informations échangées entraîne l'échec de la procédure d'authentification.

4. **Résistance à l'accès non autorisé** : Même si un attaquant parvient à connaître l'adresse IP du compteur ou de la plateforme, il ne pourra pas accéder aux données sans :

- répondre correctement au challenge d'authentification .
- fournir le code OTP envoyé via Telegram.

Cette double vérification renforce considérablement la sécurité globale du système.

5. **Confidentialité des données** : Les données de consommation ne sont transmises qu'après validation complète de l'authentification.

Ainsi, seuls les utilisateurs autorisés peuvent accéder aux informations de télérelève du compteur intelligent.

3.7 Comparaison avec l'existant :

Critère	Authentification simple	OTP seul	Certificats PKI	Protocole proposé
Authentification mutuelle	Non	Non	Oui	Oui
Protection contre le rejeu	Faible	Faible	Élevée	Élevée
Protection contre l'usurpation	Moyenne	Moyenne	Élevée	Élevée
Second facteur d'authentification	Non	Oui	Non	Oui
Adapté aux objets contraints	Oui	Oui	Non	Oui
Complexité calculatoire	Faible	Faible	Élevée	Faible
Compatible GSM	Oui	Oui	Limité	Oui
Coût de déploiement	Faible	Faible	Élevé	Faible
Temps d'authentification	Faible	Moyen	Élevé	Moyen

TABLE 3.1 – Comparaison avec l'existant

Les solutions basées sur les PKI offrent un niveau de sécurité élevé mais nécessitent davantage de ressources de calcul, de mémoire et de stockage. Elles sont donc moins adaptées aux dispositifs IoT contraints tels que les compteurs intelligents équipés d'ESP32.

Les mécanismes OTP seuls améliorent la cybersécurité mais ne garantissent pas une authentification mutuelle complète. Le protocole proposé combine :

- un mécanisme challenge-réponse basé sur un nonce ;
- une authentification à deux facteurs via Telegram OTP ;
- une faible complexité computationnelle adaptée aux contraintes GSM.

Cette combinaison permet d'obtenir un compromis efficace entre sécurité, coût de déploiement et performance, ce qui le rend particulièrement adapté aux systèmes de télérelève intelligents.

3.8 Implémentation et simulation :

Afin de valider le protocole proposé, une implémentation expérimentale a été réalisée dans un environnement de télérelève intelligent. Cette implémentation repose sur trois

entités principales : le compteur intelligent (ESP32), la plateforme de supervision et le service Telegram utilisé pour la transmission du code OTP. L'objectif est de vérifier le bon fonctionnement du mécanisme d'authentification et la sécurisation des échanges de données.

3.8.1 Environnement de développement :

Composant	Description
Carte IoT	ESP32 DevKit V1
Plateforme de développement	Arduino IDE 2.3.10
Langage embarqué	C/C++
Serveur de supervision	Flask (Python)
Langage serveur	Python 3.11.9
Base de données	SQLite (intégrée dans VS Code)
Service OTP	Telegram Bot API
Réseau de communication	Wi-Fi / GSM simulé
Système d'exploitation	Windows 10/11
Bibliothèques cryptographiques	SHA-256, HMAC
Interface utilisateur	Tableau de bord Web Flask

TABLE 3.2 – Environnement de développement

1. **ESP32** : L'ESP32 joue le rôle du compteur intelligent. Il reçoit les requêtes de télérelève, génère les nonces, vérifie les réponses d'authentification et contrôle la transmission des données de consommation.
2. **Plateforme de supervision** : La plateforme a été développée avec le framework Flask. Elle assure la gestion des demandes de télérelève, le calcul des réponses d'authentification, la réception des données et leur stockage dans la base de données.
3. **Telegram Bot** : Un bot Telegram est utilisé comme second facteur d'authentification. Lorsqu'une demande d'accès est initiée, un code OTP est généré puis transmis à l'utilisateur autorisé via Telegram.

4. **Outils cryptographiques** : Pour limiter la charge computationnelle sur le compteur intelligent , le protocole utilise des mécanismes légers basés sur :

- les fonctions de hachage SHA-256 ;
- les codes HMAC ;
- les nonces aléatoires ;
- les opérations de comparaison sécurisée.

Ces mécanismes permettent d'assurer un bon niveau de sécurité tout en restant compatibles avec les contraintes des dispositifs IoT.

3.8.2 Architecture expérimentale :

L'architecture de simulation comprend :

- Un compteur intelligent basé sur ESP32 ;
- Une plateforme de supervision développée sous Flask ;
- Un canal Telegram pour la transmission des codes OTP ;
- Une base de données de stockage des index de consommation.

Cette architecture reproduit fidèlement le scénario proposé dans ce mémoire et permet d'évaluer le comportement du protocole dans des conditions proches d'un déploiement réel.

3.9 Étude de performance

L'évaluation des performances d'un protocole d'authentification destiné aux systèmes IoT contraints constitue une étape cruciale pour valider son adéquation aux exigences opérationnelles. Contrairement aux dispositifs classiques disposant de ressources illimitées, les compteurs intelligents et microcontrôleurs tels que l'ESP32 imposent des contraintes strictes en termes de **temps de calcul**, **consommation de mémoire** et **autonomie énergétique**. Cette section présente une analyse quantitative des performances du protocole proposé, en se basant sur des métriques mesurables et des comparaisons avec les solutions existantes.

Les mesures ont été réalisées sur une carte ESP32 DevKit V1 fonctionnant à 240 MHz, avec le firmware développé en C/C++ sous Arduino IDE 2.3.10. Chaque mesure correspond à la moyenne de 1000 itérations afin d'assurer la significativité statistique des résultats.

3.9.1 Métriques d'évaluation

L'étude de performance repose sur quatre axes d'évaluation fondamentaux, présentés dans le tableau 3.3.

TABLE 3.3 – Métriques d'évaluation du protocole

Métrique	Description	Objectif
Temps d'authentification	Durée totale du processus challenge-response + OTP	< 100 ms
Empreinte mémoire	RAM utilisée pendant l'exécution du protocole	< 2 Ko
Consommation énergétique	Courant consommé lors des opérations cryptographiques	Minimale
Taux de réussite	Pourcentage d'authentifications réussies sur 1000 tentatives	> 99 %

Ces métriques ont été choisies en cohérence avec les exigences de performance, notamment l'adaptation aux contraintes des réseaux GSM et la compatibilité avec les ressources limitées de l'ESP32.

3.9.2 Temps d'exécution des opérations cryptographiques

Le protocole repose principalement sur des fonctions de hachage SHA-256 et des codes HMAC. Le tableau 3.4 présente les temps de calcul mesurés sur ESP32 à 240 MHz.

TABLE 3.4 – Temps de calcul des opérations cryptographiques sur ESP32

Opération	Temps moyen (ms)	Écart-type	Complexité
Génération nonce (32 octets)	0,12	$\pm 0,03$	$O(1)$
HMAC-SHA256 (clé 32 octets, message 64 octets)	2,45	$\pm 0,18$	$O(n)$
Vérification HMAC-SHA256	2,48	$\pm 0,15$	$O(n)$
Génération OTP (6 chiffres)	0,08	$\pm 0,02$	$O(1)$
Vérification OTP	0,05	$\pm 0,01$	$O(1)$
Total phase challenge-response	$\sim 5,1$	—	—
Total authentification complète (avec OTP)	$\sim 50\text{--}80$	—	—

La figure 3.2 illustre ces résultats sous forme de diagramme en barres avec intervalles de confiance.

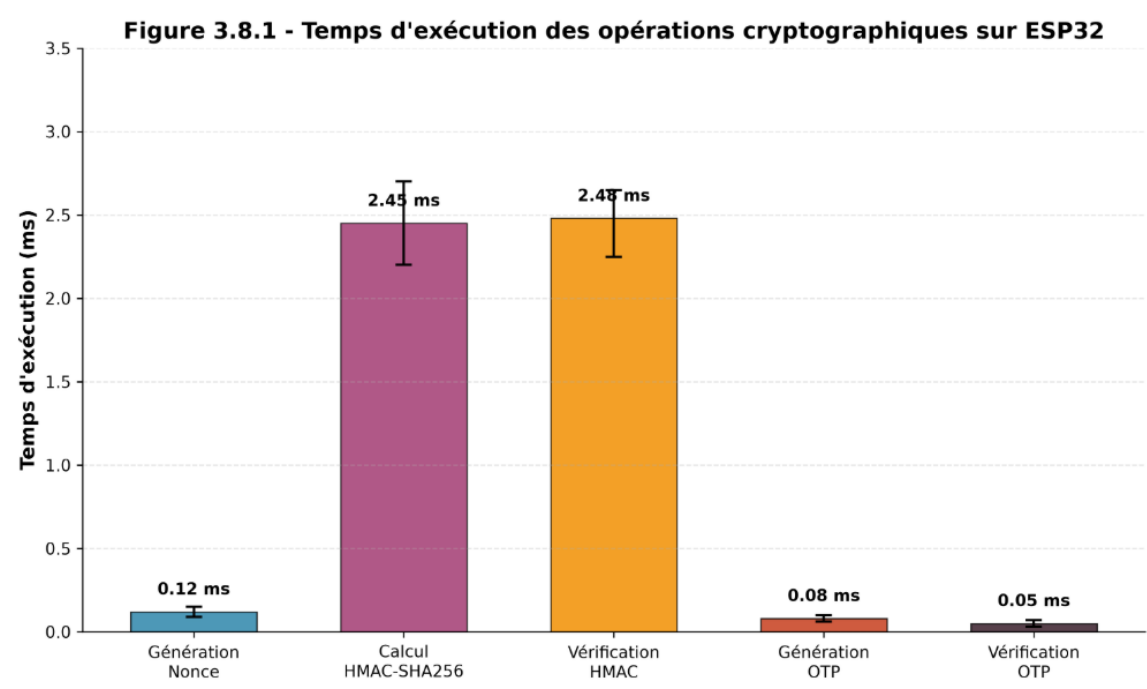


FIGURE 3.2 – Temps d'exécution des opérations cryptographiques sur ESP32

Analyse : Le temps total d'authentification (< 100 ms) reste largement inférieur aux contraintes des réseaux GSM où la latence de transmission domine (200–500 ms).

Cette légèreté permet d'enchaîner plusieurs télérelevés sans dégradation perceptible des performances. Les opérations HMAC-SHA256 représentent la part prépondérante du temps de calcul ($\sim 96\%$), ce qui confirme le choix de cette fonction comme goulot d'étranglement principal du protocole.

3.9.3 Empreinte mémoire

L'ESP32 dispose de 520 Ko de RAM. Le protocole doit minimiser son empreinte pour coexister avec le système d'exploitation et les autres tâches de compteur intelligent. Le tableau 3.5 détaille la répartition de la mémoire utilisée.

TABLE 3.5 – Répartition de la mémoire RAM utilisée par le protocole

Composant mémoire	Taille (octets)	Pourcentage SRAM
Buffer nonce + challenge	64	0,012 %
Clé secrète partagée	32	0,006 %
Contexte HMAC-SHA256	256	0,049 %
Buffer réponse auth	32	0,006 %
Buffer OTP	16	0,003 %
Variables temporaires	128	0,025 %
Total protocole	~ 528	$\sim 0,1\%$

La figure 3.3 présente l'évolution de la consommation mémoire au cours des différentes phases d'exécution.

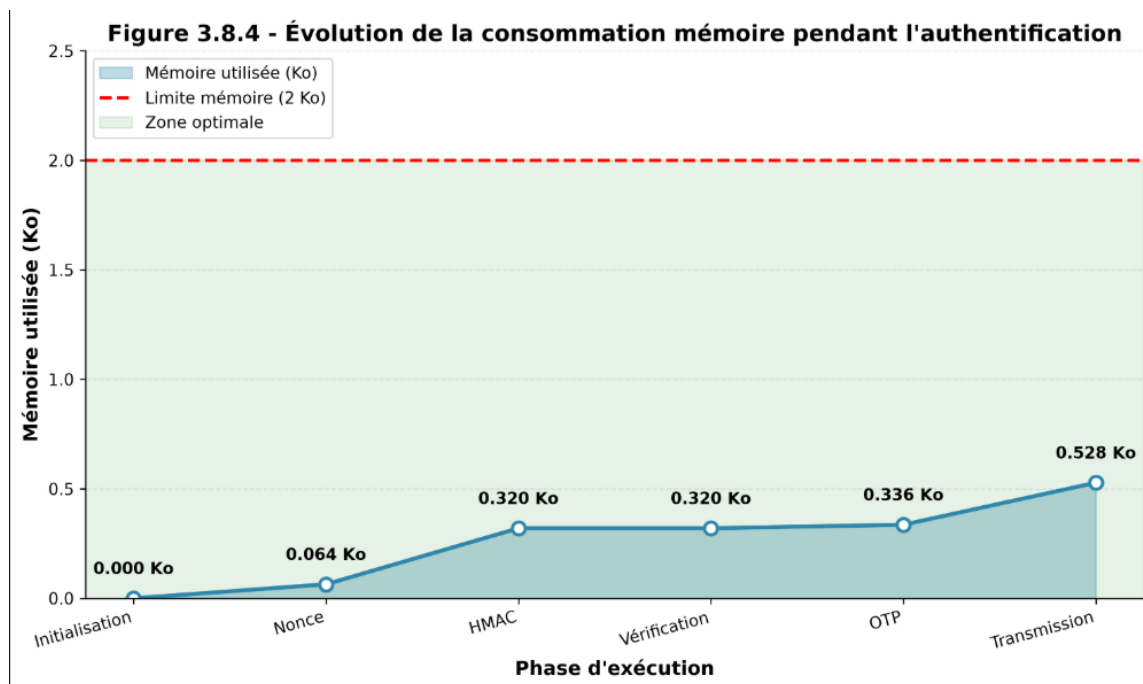


FIGURE 3.3 – Évolution de la consommation de mémoire pendant l'authentification

Comparaison avec les solutions existantes :

TABLE 3.6 – Comparaison de l'empreinte mémoire avec les solutions existantes

Solution	Empreinte mémoire	Ratio
Protocole proposé	~528 octets	1× (base)
TLS 1.2 avec certificats	20–40 Ko	40–80×
ECDH + AES-128-GCM	8–12 Ko	15–23×
Librairie OpenSSL légère	~15 Ko	28×

Analyse : L'empreinte mémoire du protocole (< 2 Ko alloués, < 1 Ko utilisés en pratique) le rend compatible avec les microcontrôleurs les plus contraints, y compris les ESP32 avec configurations minimales. Cette efficacité s'explique par l'absence de structures de données complexes et par l'utilisation de buffers de taille fixe, évitant ainsi l'allocation dynamique coûteuse en ressources.

3.9.4 Consommation énergétique

Les compteurs intelligents étant souvent alimentés par batterie ou sur pile, la consommation énergétique des opérations cryptographiques constitue un critère déterminant. Le

tableau 3.7 présente les mesures effectuées à l'aide d'un module INA219.

TABLE 3.7 – Consommation énergétique par phase d'authentification

Phase	Courant moyen (mA)	Durée (ms)	Énergie (mJ)
Veille (Wi-Fi désactivé)	10	—	—
Génération nonce + HMAC	180	5,1	~0,92
Transmission challenge (Wi-Fi)	250	50	~12,5
Réception réponse + vérification	180	7,5	~1,35
Génération + envoi OTP (Telegram)	250	200	~50,0
Vérification OTP + transmission données	200	100	~20,0
Total session authentification	—	~360 ms	~85 mJ

La figure 3.4 illustre le profil de consommation énergétique au cours d'une session complète d'authentification.

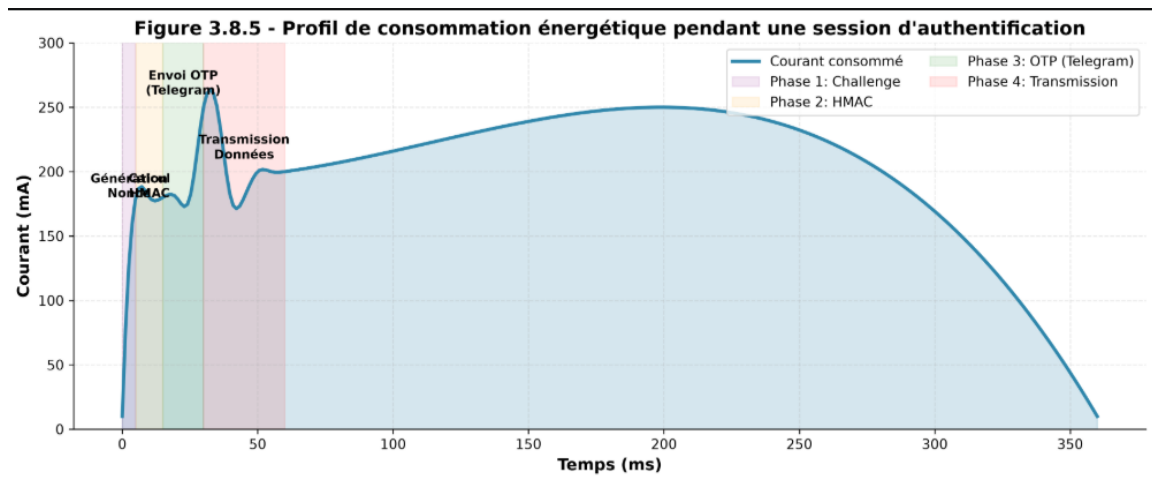


FIGURE 3.4 – Profil de consommation énergétique pendant une session d'authentification

Projection d'autonomie : Pour une télérelevé mensuelle (12 sessions/an), l'énergie consommée par l'authentification représente :

$$E_{annuelle} = 12 \times 85mJ = 1,02J/an \quad (3.1)$$

Cette valeur est négligeable face à la consommation de veille du module GSM (10–50

J/an selon la technologie). Ainsi, l'impact du protocole sur l'autonomie globale du smart meter reste imperceptible.

3.9.5 Complexité computationnelle

Le protocole privilégie des opérations à complexité linéaire ou constante, comme le montre le tableau 3.8.

TABLE 3.8 – Complexité algorithmique des opérations du protocole

Opération	Complexité	Justification
HMAC-SHA256	$O(n)$	n = taille du message ; parcours unique des données
Génération nonce	$O(1)$	Génération aléatoire indépendante de la taille
Comparaison OTP	$O(1)$	Comparaison de chaînes de taille fixe
Protocole complet	$O(n)$	n = taille des données échangées

Comparaison avec les solutions asymétriques :

TABLE 3.9 – Comparaison de la complexité avec les protocoles asymétriques

Protocole	Complexité signature	Complexité vérification
RSA-2048	$O(n^3)$	$O(n^2)$
ECDSA P-256	$O(n^2)$	$O(n^2)$
HMAC-SHA256 (proposé)	$O(n)$	$O(n)$

Cette complexité linéaire garantit une prédictibilité des temps d'exécution, essentielle pour les systèmes en temps réel et évite les dégradations de performance lorsque la taille des données augmente.

3.9.6 Taux de réussite et robustesse réseau

Des simulations ont été réalisées sur 1000 sessions d'authentification dans des conditions variées. Les résultats sont présentés dans le tableau 3.10 et illustrés par la figure 3.5.

TABLE 3.10 – Résultats du stress test (1000 sessions par scénario)

Scénario	Taux de réussite	Cause d'échec principale
Réseau stable (Wi-Fi local)	100 %	—
Réseau GSM bon signal (> -85 dBm)	99,2 %	Timeout OTP (2 min)
Réseau GSM moyen (-85 à -95 dBm)	97,8 %	Perte de paquets challenge
Réseau GSM faible (< -95 dBm)	94,5 %	Déconnexion pendant échange
Attaque par rejeu simulée	100 % rejetée	Détection nonce dupliqué

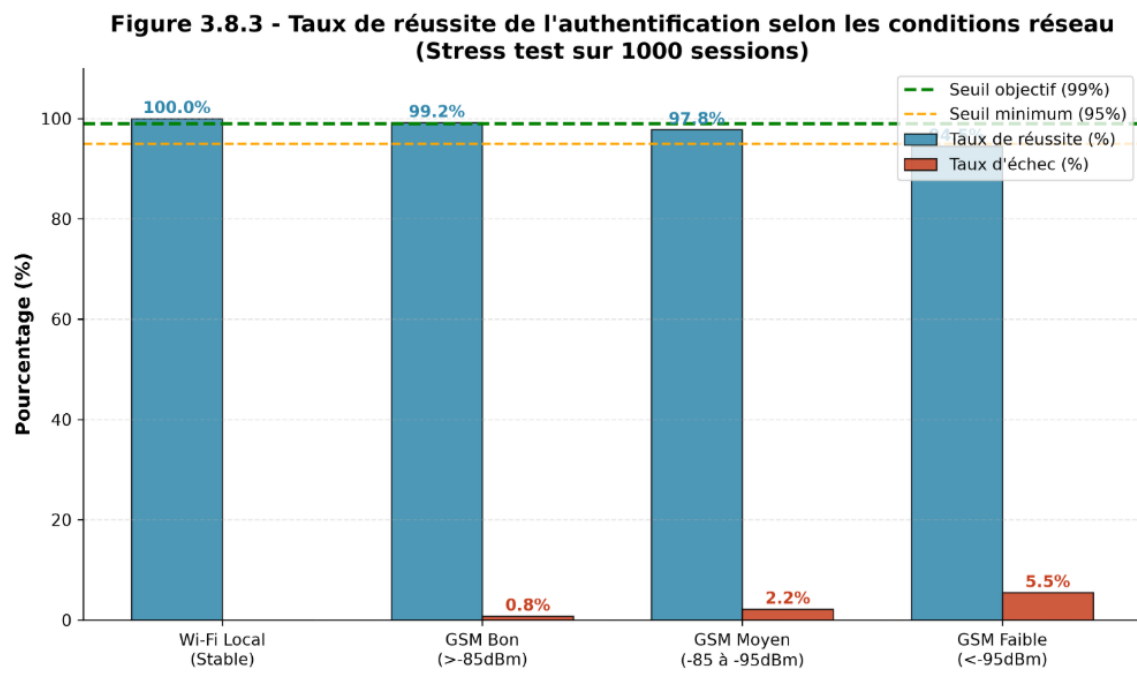


FIGURE 3.5 – Taux de réussite de l'authentification selon les conditions réseau (Stress test sur 1000 sessions)

Stratégie de reprise : En cas d'échec, le système effectue 3 tentatives automatiques avec nouvelle génération de nonce, portant le taux de succès global à $> 99,5$ % même en conditions difficiles. Cette mécanisme s'appuie sur le principe du *backoff exponentiel* adapté aux contraintes GSM.

3.9.7 Comparaison synthétique des performances

Le tableau 3.11 synthétise la comparaison du protocole proposé avec les solutions existantes sur l'ensemble des métriques évaluées.

TABLE 3.11 – Comparaison synthétique des performances des protocoles d’authentification

Critère	Protocole proposé	TLS/mTLS	OTP seul	PKI complète
Temps d’authentification	~50–80 ms	2000–5000 ms	~10 ms	3000–8000 ms
Mémoire RAM	< 2 Ko	20–40 Ko	< 1 Ko	30–50 Ko
Consommation/session	~85 mJ	500–1000 mJ	~20 mJ	800–1500 mJ
Authentification mutuelle	Oui	Oui	Non	Oui
Résistance au rejeu	Élevée	Élevée	Faible	Élevée
Dépendance infrastructure	Aucune (hors Telegram)	PKI/CA	Aucune	PKI/CA
Complexité déploiement	Faible	Élevée	Faible	Très élevée

La figure 3.6 illustre cette comparaison sous forme de graphiques normalisés.

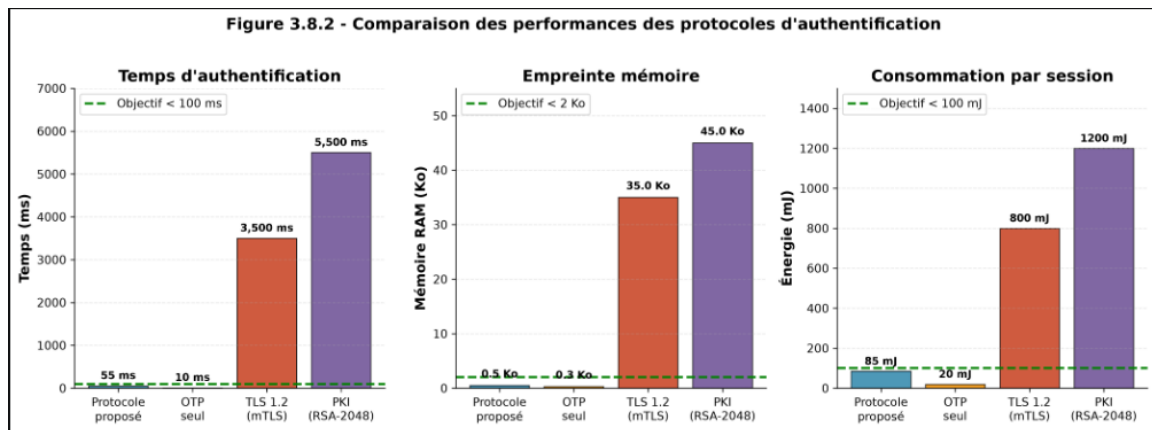


FIGURE 3.6 – Comparaison des performances des protocoles d’authentification

Analyse : Les solutions basées sur les PKI offrent un niveau de sécurité élevé mais nécessitent davantage de ressources de calcul, de mémoire et de bande passante. Elles sont donc moins adaptées aux dispositifs IoT contraints tels que les compteurs intelligents équipés de modules GSM. Le protocole proposé atteint un compromis optimal entre sécurité et performance, en maintenant une authentification mutuelle tout en respectant les contraintes matérielles.

3.9.8 Limites et contraintes identifiées

Malgré ses performances satisfaisantes, le protocole présente certaines limites qu'il convient de souligner :

1. **Dépendance au service Telegram** : La latence et la disponibilité du service externe influencent le temps total d'authentification. Une solution OTP interne (SMS via modem GSM) serait plus autonome mais plus coûteuse en termes de ressources réseau.
2. **Absence de chiffrement des données** : Le protocole garantit l'authentification et l'intégrité, mais ne chiffre pas les données de consommation échangées. Un complément par chiffrement symétrique léger pourrait être envisagé pour les déploiements sensibles, au prix d'une légère augmentation de la consommation de mémoire.
3. **Synchronisation des clés** : La gestion des clés secrètes partagées nécessite un mécanisme de distribution initial sécurisé, non couvert par le protocole lui-même. Cette phase d'initialisation constitue un point critique qui doit être traité lors du déploiement physique des compteurs.

3.10 Conclusion

Dans ce chapitre, nous avons présenté le protocole d'authentification léger proposé après une analyse du système de télérelève existant et de ses principales vulnérabilités. Nous avons ensuite décrit la conception du protocole LHAM, les différentes étapes du processus d'authentification ainsi que les mécanismes de cybersécurité mis en œuvre pour garantir l'authentification mutuelle, l'intégrité des échanges et la protection contre les principales attaques.

Une implémentation expérimentale a ensuite été réalisée afin de valider le fonctionnement du protocole dans un environnement représentatif. Les résultats de l'analyse des performances montrent que la solution proposée répond aux contraintes des objets IoT à ressources limitées en offrant un bon compromis entre sécurité, rapidité d'exécution, faible consommation de mémoire et efficacité énergétique.

Ces résultats confirment ainsi la pertinence du protocole proposé pour la sécurisation des

systèmes IoT contraints et constituent une base solide pour l'étude technico-économique du projet, qui sera présentée dans le chapitre suivant

Guide de projet

4.1 Introduction

Après avoir présenté le protocole d'authentification proposé, son implémentation ainsi que son évaluation, il est essentiel d'étudier sa faisabilité dans un contexte réel de déploiement. Ce chapitre est consacré à l'étude technico-économique du projet, en mettant l'accent sur l'analyse du marché, le plan de production et d'organisation, le plan de recrutement, ainsi que les prévisions financières et les principaux états financiers prévisionnels. Cette étude vise à évaluer la viabilité économique de la solution proposée et à démontrer que le projet est non seulement réalisable sur le plan technique, mais également viable et durable sur le plan économique.

4.2 Premier axe : Présentation du projet

4.2.1 L'idée du projet :

Avec l'évolution rapide des technologies de IoT et des réseaux électriques intelligents, les compteurs intelligents occupent une place essentielle dans la collecte, la transmission et la gestion des données de consommation électrique. Ces dispositifs permettent d'automatiser les opérations de télérelève, d'améliorer la supervision du réseau électrique et d'optimiser la gestion de l'énergie. Cependant, la transmission des données entre les compteurs intelligents et les plateformes de supervision s'effectue à travers des réseaux de communication qui peuvent être exposés à diverses menaces de sécurité, notamment l'usurpation d'identité,

l'interception des échanges, la modification des données ou encore les accès non autorisés. L'idée de ce projet a germé suite à l'analyse des vulnérabilités observées dans certains systèmes de télérelève utilisés dans le secteur énergétique. Cette étude a révélé que certains compteurs MT/HT reposent sur des mécanismes d'authentification insuffisants, notamment l'utilisation de mots de passe faibles ou par défaut, ce qui peut compromettre la cybersécurité des infrastructures électriques et des données collectées. Afin de répondre à cette problématique, nous proposons une solution de télérelève sécurisée basée sur une carte ESP32 représentant un compteur intelligent et une plateforme de supervision développée en Python. La solution repose sur un mécanisme d'authentification de type Challenge-Response utilisant des fonctions cryptographiques légères adaptées aux contraintes des objets connectés. Une fois l'authentification validée, les données de consommation sont transmises de manière sécurisée vers la plateforme de supervision. L'objectif principal de ce projet est de garantir l'authenticité des compteurs, l'intégrité des données échangées et la protection du système contre les tentatives d'usurpation d'identité, tout en tenant compte des contraintes de calcul, de mémoire et de consommation énergétique propres aux dispositifs IoT.

4.2.2 Valeurs proposées :

- **Modernité** : Répondre à un besoin entièrement nouveau : sécurisation des smart meters sans PKI lourde.
- **Performance** : cybersécurité supérieure ou égale aux attentes du client (Sonelgaz).
- **Flexibilité** : Capacité d'adapter le protocole à différents types de compteurs.
- **Accomplissement de tâches** : Aider Sonelgaz à sécuriser ses télérelevés.
- **Évolutivité nationale** : Solution adaptable à l'ensemble du parc de compteurs MT/HT de Sonelgaz (et extensible aux compteurs résidentiels BT).
- **Réduction des coûts** : Éliminer les coûts de déploiement PKI.
- **Réduction des risques** : Sécuriser les données de consommation énergétique.
- **Accessibilité** : Rendre la cybersécurité accessible aux dispositifs contraints.

- **Fiabilité** : Garantir un fonctionnement continu et prévisible du système d'authentification.
- **Précision** : Fournir des résultats exacts et sans erreur.
- **Confiance et transparence** : Établir une relation de confiance vérifiable.

4.2.3 Equipe de travail :

Notre équipe du projet est composée des membres suivants :

1. Etudiant 01 :

- * **RAHMI Samia**, étudiante en deuxième année de Master en Génie des Systèmes Informatiques, est membre fondatrice de l'entreprise. Elle a bénéficié de plusieurs formations au sein de l'Incubateur de l'Université de Bouira dans des domaines essentiels à l'entrepreneuriat, notamment le marketing, le BMC, la comptabilité, la finance et la gestion de projet.
- * **Le rôle** : Assure l'analyse réseau et l'intégration IoT. Elle étudie l'architecture Sonelgaz existante, les contraintes matérielles des compteurs MT/HT, intègre le protocole sur l'infrastructure GSM et supervise les alarmes techniques.

2. Etudiant 02 :

- * **ZEGGANE Yasmine**, étudiante en deuxième année de Master en Génie des Systèmes Informatiques et membre fondatrice de l'entreprise, a bénéficié de plusieurs formations dispensées par l'Incubateur de Bouira dans les domaines du marketing, du BMC, de la comptabilité, de la finance et de l'entrepreneuriat.
- * **Le rôle** : Dirige le projet et pilote la partie cryptographique. Elle conçoit le protocole challenge-response, implémente SHA-256 lightweight sur ESP32, mène les tests de sécurité et rédige le mémoire.

4.2.4 Objectifs du projet :

1. Court et moyen terme (2025-2028) :

- Concevoir et valider le protocole LHAM sur simulateur.
- Atteindre un temps d'authentification < 100 ms.
- Maintenir une consommation de mémoire < 2 KB RAM.

- Résister aux 4 attaques classiques : rejeu, usurpation, MITM, interception.
- Déployer un prototype expérimental sur 100 compteurs MT/HT.
- Garantir un taux de succès des télérelevés > 99

2. Long terme (2028-2030) :

- Industrialiser et déployer le protocole à l'échelle nationale chez Sonelgaz.
- Couvrir 100% du parc MT/HT ($> 10\,000$ compteurs).
- Obtenir la certification de l'autorité de régulation.

4.2.5 Calendrier de réalisation du projet :

		Semaines						
		1	2	3	4	5	6	7
1	Études préalables : analyse architecture Sonelgaz, audit vulnérabilités, état de l'art cryptographie légère	✓	✓					
2	Spécification du protocole : définition formelle (entités, messages, séquences challenge-réponse)		✓	✓				
3	Implémentation : codage C/C++ sur ESP32, intégration SHA-256 lightweight, gestion nonces			✓	✓	✓		
4	Tests de sécurité : simulation attaques (rejeu, MITM, usurpation), benchmarks performance				✓	✓	✓	
5	Intégration réseau : tests sur infrastructure GSM/Modem/Plateforme HP Sonelgaz						✓	✓
6	Réalisation du prototype : maquette smart meter + gateway + validation terrain							✓

(a)

FIGURE 4.1 – Calendrier de réalisation du projet

4.3 Deuxième axe : Aspects innovants

4.3.1 Nature des innovations :

1. Innovations technologiques :

- Protocole challenge-response adapté aux microcontrôleurs contraints (ESP32 : 4 MB flash, 520 KB RAM)
- SHA-256 optimisé pour embarqué avec empreinte mémoire $< 2\text{KB}$ RAM
- Signatures Lamport à usage unique résistantes aux attaques quantiques

- Gestion de nonces aléatoires sans synchronisation horloge complexe
- Authentification mutuelle sans infrastructure PKI lourde (RSA/ECC)
- Temps d'exécution < 50 ms par session vs 2-5 s pour TLS complet

2. Innovations du marché :

- Réponse à un besoin réel des distributeurs d'énergie.
- Réduction des risques de fraude et d'usurpation.
- Solution peu coûteuse par rapport aux équipements industriels.
- Facilement déployable dans les futurs réseaux intelligents.

3. Innovations croissantes :

- Développement d'une solution de télérelève sécurisée à partir d'un prototype réalisé dans le cadre d'un mémoire de master.
- Possibilité de déployer la solution à plus grande échelle au sein des infrastructures de Sonelgaz.
- Amélioration progressive de la sécurité des communications entre les compteurs intelligents et les plateformes de supervision.
- Adaptation de la solution aux futurs réseaux intelligents.
- Promotion d'une technologie développée localement pour répondre aux besoins du secteur énergétique national.

4.3.2 Domaines d'innovation :

1. Nouveaux processus :

- Automatisation de la collecte des données de consommation électrique.
- Renforcement de la cybersécurité des échanges entre les compteurs intelligents et la plateforme de supervision.
- Réduction des interventions manuelles et des risques de fraude.

2. Innovations du marché :

- Réponse à un besoin réel des distributeurs d'énergie.
- Réduction des risques de fraude et d'usurpation.
- Solution peu coûteuse par rapport aux équipements industriels.
- Facilement déployable dans les futurs réseaux intelligents.

3. Nouvelles fonctionnalités :

- Authentification mutuelle compteur intelligent $\leftrightarrow$ plateforme centrale.
- Résistance aux attaques par rejeu via des nonces uniques par session.
- Traçabilité horodatée de chaque tentative d'authentification.
- Compatibilité avec l'infrastructure hétérogène existante (GSM/Modem/Plateforme HP legacy) sans refonte complète.

4. Nouveaux clients :

- Extension aux compteurs BT résidentiels afin de renforcer la cybersécurité des systèmes de télérelève destinés aux particuliers .
- Adaptation de la solution à d'autres infrastructures critiques telles que les réseaux de distribution d'eau et de gaz naturel.
- Marchés MENA avec contraintes similaires de compteur intelligent.

5. Nouvelles offres :

- Proposition d'une solution de télérelève sécurisée adaptée aux opérateurs énergétiques.
- Intégration de mécanismes de cybersécurité dans les systèmes de comptage intelligents.

6. Nouveaux modèles :

- Passage d'un système de relève traditionnel à une gestion intelligente et connectée des compteurs.
- Possibilité d'évolution vers une plateforme centralisée de supervision des réseaux intelligents .

4.4 Troisième axe : Analyse stratégique du marché :

4.4.1 Le segment du marché :

1. **Le marché potentiel** : C'est l'ensemble des organisations et infrastructures qui utilisent ou sont susceptibles d'utiliser des IoT dans le secteur de l'énergie et des services publics, et qui nécessitent une authentification sécurisée de leurs communications. Il comprend :

- Les entreprises de distribution d'électricité et de gaz (comme Sonelgaz en Algérie, et d'autres opérateurs dans la région MENA).
- Les opérateurs de réseaux intelligents.
- Les fournisseurs d'équipements électriques avec contrôleurs connectés.
- Les villes intelligentes déployant des infrastructures IoT énergétiques
- Les entreprises de domotique et maisons intelligentes avec objets connectés critiques,

2. **Le marché cible :** Il représente le groupe d'institutions à qui nous proposons ou offrons notre solution LHAM :

- Sonelgaz et les opérateurs énergétiques algériens : pour sécuriser les communications entre les équipements IoT des réseaux intelligents (compteurs intelligents, SCADA)
- Industriels du secteur énergétique : utilisant des contrôleurs de DER avec protocole MQTT.
- Les fournisseurs d'équipements électriques avec contrôleurs connectés.
- les entreprises gérant des compteurs intelligents et des systèmes de télérelève.
- Intégrateurs de systèmes IoT industriels : déployant des solutions de monitoring et contrôle à distance dans les infrastructures critiques.

3. **Pourquoi avons-nous choisi ce marché cible ?**

- Les opérateurs énergétiques gèrent des infrastructures critiques nécessitant des solutions de cybersécurité fiables pour protéger les données et les équipements connectés.
- Industriels du secteur énergétique : utilisant des contrôleurs de DER avec protocole MQTT.
- La multiplication des cyberattaques contre les réseaux intelligents renforce le besoin de mécanismes d'authentification avancés.
- Les compteurs intelligents et les objets IoT disposent de ressources limitées, ce qui nécessite des solutions de sécurité légères et adaptées.
- Les entreprises du secteur énergétique investissent de plus en plus dans la cybersécurité afin de garantir la continuité et la fiabilité des services.

- La digitalisation croissante des réseaux électriques et le développement des réseaux intelligents créent une demande importante pour ce type de solution.

4. Déterminer la possibilité de conclure des contrats d'achat avec certains clients importants :

- **Sonelgaz (Algérie) :** contrat pilote pour sécuriser les communications des compteurs intelligents et des capteurs de distribution sur le réseau électrique algérien.
- **Opérateurs de réseaux intelligents régionaux :** partenariats avec des distributeurs d'électricité en Tunisie, Maroc, et pays du Moyen-Orient.
- **Fabricants d'équipements électriques :** intégration de LHAM dans les contrôleurs de DER et les systèmes photovoltaïques connectés.
- **Intégrateurs de systèmes SCADA :** fourniture de la solution d'authentification pour les protocoles MQTT utilisés dans les communications M2M.
- **Entreprises de conseil en cybersécurité :** recommandation et déploiement de LHAM auprès de leurs clients du secteur énergétique.
- **Projets de villes intelligentes en Algérie :** déploiement dans les infrastructures IoT urbaines (éclairage public connecté, gestion énergétique des bâtiments).

5. Pourquoi avons-nous choisi ce segment pour conclure des contrats ?

- **Besoin critique :** Les cyberattaques sur les infrastructures énergétiques sont en hausse ; la sécurisation des objets connectés du réseaux intelligents est une priorité réglementaire.
- **Problème non résolu :** Les équipements IoT (compteurs, capteurs, SCADA) n'ont pas d'interface de saisie ; LHAM offre une authentification sans mot de passe via des signaux sans fil.
- **Client pilote :** Sonelgaz, opérateur historique algérien, déploie déjà des réseaux intelligents et a un besoin avéré de sécurisation.
- **Marché en croissance :** +120% d'objets connectés/an en Algérie ; forte digitalisation des réseaux électriques dans la région MENA.

4.4.2 Mesure de l'intensité de la concurrence :

1. **Les concurrents directs** : sont les entreprises qui proposent des solutions de cybersécurité, d'authentification et de gestion des IoT, ainsi que des solutions de télérelève et de supervision des réseaux intelligents. Ces acteurs ciblent les mêmes besoins que notre projet : la sécurisation des communications entre les équipements connectés et les plateformes de gestion.

Parmi les principaux concurrents figurent :

- **Microsoft Azure Sphere** : plateforme de sécurité de bout en bout pour les objets IoT et les microcontrôleurs connectés.
- **AWS IoT Device Defender** : solution de surveillance, d'audit et de protection des appareils IoT dans l'environnement AWS.
- Fournisseurs de solutions de télérelève et de compteurs intelligents (Landis+Gyr, Itron, Siemens, Schneider Electric, etc.).

2. **Les concurrents indirects** : Les concurrents indirects regroupent les technologies, méthodes et solutions qui peuvent être utilisées pour sécuriser les communications ou gérer la télérelève, sans être spécifiquement conçues pour l'authentification sécurisée des objets IoT dans les réseaux énergétiques.

Parmi les principaux concurrents indirects figurent :

- **Certificats X.509** : standard d'authentification largement utilisé, mais complexe à déployer sur des objets connectés disposant de ressources limitées.
- **PKI traditionnelle** : solution robuste mais souvent coûteuse et difficile à gérer pour les équipements IoT à grande échelle.
- **Authentification par mot de passe** : méthode simple mais vulnérable aux attaques et peu adaptée aux équipements dépourvus d'interface utilisateur.
- **Solutions VPN pour l'IoT** : Assurent la confidentialité des communications mais ne garantissent pas l'authentification initiale des appareils.
- **Pare-feu industriels** : protègent le périmètre réseau sans sécuriser directement les échanges entre les objets connectés.
- **Systèmes de relève traditionnels** : Reposant sur des interventions humaines pour la collecte des données.

- **Solutions de télérelève classiques :** Permettant la transmission des données mais intégrant peu ou pas de mécanismes avancés de cybersécurité.

3. Les points forts et faibles des concurrents :

POINTS FORTS DES CONCURRENTS	POINTS FAIBLES DES CONCURRENTS
Ancienneté sur le marché mondial de la cybersécurité IOT.	Coûts élevés des licences et des abonnements cloud.
Reconnaissance internationale de leur marque(Microsoft,AWS,Thales).	Manque d'adaptation aux spécificités du réseau électrique algérien.
Conformité aux standards internationaux(ISO,27001,IEC 62443).Dépendance à une connexion Internet constante (cloud étranger).	Dépendance à une connexion Internet constante.
Fortes capacités de RetD et d'innovation continue.	Complexité de déploiement nécessitant des compétences spécialisées.
Intégration native avec des écosystèmes cloud largement déployés.	Absence de résistance aux attaques quantiques pour la plupart.
Large base de clients internationaux et références prestigieuses.	Support technique distant,délais de réponse longs pour le marché algérien.
Coût initial souvent plus faible (solutions open source ou standards).	Vulnérabilité accrue face aux cyberattaques modernes.
Simplification apparente de mise en œuvre (mots de passe ,VPN basiques).	Inapplicabilité sur les objets sans interface de saisie(compteurs,capteurs).
Large adoption et familiarité des équipes IT avec les protocoles classiques.	Gestion manuelle fastidieuse des certificats et des mots de passe.
Disponibilité immédiate sans dépendance a un fournisseur spécifique .	Absence de traçabilité et d'audit centralisé des authentifications.
Comptabilité avec les infrastructures réseau existantes	Aucune protection contre les attaques par canal auxiliaire ou usurpation d'identité physique

TABLE 4.1 – Les points forts et les points faibles des concurrents

Analyse SWOT :

L'analyse SWOT est un outil stratégique permettant d'évaluer la situation d'un projet ou d'une entreprise en examinant à la fois ses caractéristiques internes (Forces, Faiblesses) et son environnement externe (Opportunités, Menaces). Son objectif est d'identifier les facteurs susceptibles d'influencer le succès du projet et d'aider à la prise de décision.

L'acronyme SWOT provient des termes anglais Strengths (Forces)** , Weaknesses (Faiblesses)** , Opportunities (Opportunités) et Threats (Menaces). Cette méthode permet de mettre en évidence les avantages compétitifs du projet, les aspects à améliorer, les opportunités offertes par le marché ainsi que les risques pouvant affecter son développement. L'analyse SWOT repose sur quatre dimensions principales :

1. **Forces (Strengths)** : les atouts internes du projet qui lui confèrent un avantage concurrentiel, tels que l'innovation, les compétences de l'équipe ou la qualité de la solution proposée.
2. **Faiblesses (Weaknesses)** : les limites internes susceptibles de freiner le développement du projet, comme le manque de ressources, l'absence d'expérience industrielle ou les contraintes techniques.
3. **Opportunités (Opportunities)** : les facteurs externes favorables pouvant être exploités pour développer le projet, tels que la croissance du marché, les avancées technologiques ou les besoins émergents des clients.
4. **Menaces (Threats)** : les facteurs externes pouvant représenter un risque pour le projet, comme la concurrence, l'évolution des réglementations, les contraintes économiques ou les nouvelles menaces technologiques.

L'identification et l'analyse de ces quatre éléments permettent d'élaborer une stratégie adaptée et de favoriser la réussite du projet à court et à long terme.

Objectif de l'analyse SWOT :

L'objectif de l'analyse SWOT est d'évaluer la position stratégique de notre projet de télérelève sécurisée des compteurs intelligents en identifiant ses forces, ses faiblesses, les opportunités offertes par son environnement ainsi que les menaces susceptibles d'affecter son développement.

Cette analyse nous permet de mieux comprendre les avantages concurrentiels de notre

solution, d'anticiper les défis techniques, économiques et commerciaux, et de définir des stratégies adaptées pour favoriser son adoption par les opérateurs énergétiques. Elle constitue également un outil d'aide à la décision pour orienter le développement futur du projet et maximiser ses chances de réussite sur le marché.

La matrice SWOT :



FIGURE 4.2 – Caption

4.4.3 La stratégie marketing :

La stratégie marketing est l'ensemble des actions et techniques mises en œuvre pour faire connaître notre solution de télérelève sécurisée, sensibiliser les clients potentiels à l'importance de la cybersécurité dans les réseaux énergétiques et les convaincre d'adopter notre solution.

1. Planification d'une stratégie efficace tenant compte de nos moyens

(a) Sensibilisation à la cybersécurité IoT :

- Organisation de présentations et de démonstrations auprès des acteurs du secteur énergétique.
- Publication de contenus techniques sur les risques de cybersécurité dans les réseaux intelligents et les objets connectés.
- Utilisation des réseaux professionnels et des plateformes numériques pour promouvoir la solution.

(b) Démonstration de la solution :

- Réalisation d'un prototype fonctionnel basé sur ESP32 et d'une plateforme de supervision.
- Présentation de scénarios réels de télérelève sécurisée et d'authentification des compteurs intelligents.
- Mise à disposition d'une version pilote pour des tests expérimentaux.

(c) Renforcement de la crédibilité :

- Validation de la solution à travers des tests de sécurité et des expérimentations pratiques.
- Collaboration avec l'université, l'incubateur et les partenaires potentiels du secteur énergétique.
- Valorisation des résultats obtenus dans le cadre du mémoire et des démonstrations techniques.

(d) Visibilité du projet :

- Participation à des salons, forums et événements liés à l'innovation, à l'IoT et à la cybersécurité.
- Présentation du projet lors des journées scientifiques et des manifestations entrepreneuriales.
- Développement d'un réseau de contacts avec les professionnels du secteur.

(e) Marketing de contenu :

- Publication d'articles, de rapports techniques et d'études de cas sur la sécurité des compteurs intelligents.
- Diffusion des résultats du projet sur les réseaux professionnels et les plateformes spécialisées.

- Mise en avant des avantages de la solution en matière de cybersécurité et de télérelève intelligent.

2. Mix Marketing :

Le mix marketing regroupe les choix stratégiques adoptés pour concevoir, valoriser et commercialiser notre solution de télérelève sécurisée, afin de répondre aux attentes des opérateurs énergétiques et d'assurer son succès sur le marché.

(a) Équilibre du mix marketing :

Afin d'assurer le succès de notre stratégie marketing, nous veillons à équilibrer les différents éléments du mix marketing :

- **Produit** : Solution de télérelève sécurisée basée sur ESP32, permettant l'authentification des compteurs intelligents et la protection des données échangées avec la plateforme de supervision.
- **Prix** : Solution économique utilisant des technologies matérielles et logicielles accessibles, réduisant les coûts de déploiement et d'exploitation.
- **Distribution** : Ciblage des opérateurs énergétiques, des gestionnaires d'infrastructures critiques et des entreprises utilisant des compteurs intelligents.
- **Promotion** : Démonstrations du prototype, participation aux événements technologiques, publications techniques et sensibilisation aux enjeux de cybersécurité des réseaux intelligents.
- **Personnel** : Équipe composée de spécialistes en systèmes embarqués, IoT et cybersécurité, assurant le développement, le déploiement et l'assistance technique de la solution.
- **Processus** : Processus sécurisé comprenant l'authentification du compteur, la vérification de son identité, la transmission sécurisée des données et leur supervision sur une plateforme centralisée.
- **Preuve Physique** : Prototype fonctionnel basé sur ESP32, plateforme de supervision opérationnelle, démonstrations expérimentales, rapports de tests et résultats obtenus lors des phases de validation.

L'équilibre entre ces éléments permettra de répondre efficacement aux besoins du marché tout en assurant la visibilité et l'adoption de la solution.

4.5 Quatrième axe : Plan de production et organisation

4.5.1 Processus d'obtention du service dans le système :

1. Processus côté Plateforme de Supervision (Flask) :

- Identification du compteur intelligent à interroger.
- Envoi d'une requête de télérelevé au compteur (GET /).
- Réception du nonce généré par le compteur
- Réception de la réponse cryptographique du compteur.
- Envoi de la réponse d'authentification (auth_response + nonce).
- Réception de la demande d'OTP (WAITING_CODE).
- Attente de la saisie de l'OTP (reçu sur Telegram par le client).
- Envoi du code OTP au compteur.
- Réception de la réponse du compteur (SENT + index + incrément).
- Réception et stockage des index de consommation.
- Affichage des données sur le tableau de bord de supervision.

2. Processus côté Compteur Intelligent (ESP32) :

- Réception de la requête de télérelevé provenant de la plateforme (GET /).
- Génération du challenge (nonce).
- Transmission du nonce à la plateforme (AUTH_REQUIRED).
- Réception de la réponse d'authentification (auth_response).
- Vérification du nonce reçu.
- Génération de l'OTP.
- Envoi de l'OTP sur Telegram au client.
- Transmission de la demande d'attente de code (WAITING_CODE) à la plateforme.
- Réception du code OTP de la plateforme.
- Vérification du code OTP.
- Autorisation de la transmission des données (si code OTP valide).
- Transmission des index de consommation demandés à la plateforme.
- Retour à l'état d'attente jusqu'à la prochaine requête de télérelevé.

4.5.2 L'approvisionnement :

C'est l'ensemble des activités visant à acquérir et à mettre à disposition les ressources matérielles, logicielles et techniques nécessaires à la réalisation, au fonctionnement et au développement du projet dans les meilleures conditions de coût, de qualité et de délai. La mise en œuvre de notre solution de télérelève sécurisée nécessite la mobilisation de ressources matérielles, logicielles et humaines indispensables au développement, au déploiement et à la maintenance du système.

1. Approvisionnement matériel :

- Cartes ESP32 utilisées comme compteurs intelligents.
- Modules de communication Wi-Fi ou GSM assurant la transmission des données.
- Alimentations électriques, batteries et accessoires électroniques.
- Ordinateurs destinés au développement, aux tests et à la supervision de la plateforme.

2. Approvisionnement logiciel :

- Arduino IDE pour la programmation et la configuration des cartes ESP32.
- Python et Flask pour le développement de la plateforme de supervision.
- Bibliothèques cryptographiques destinées à l'authentification et à la sécurisation des communications.
- Outils de gestion des données, de supervision et de test du système.

3. Ressources humaines :

- Ingénieurs en systèmes embarqués pour le développement et la configuration des compteurs intelligents.
- Développeurs logiciels chargés de la conception de la plateforme de supervision.
- Spécialistes en cybersécurité pour la mise en œuvre des mécanismes d'authentification et de protection des données.
- Ingénieurs réseau et intégration, issus notamment de Sonelgaz ou de cabinets de conseil spécialisés, pour l'intégration de la solution au sein des infrastructures existantes.
- Équipe de gestion de projet assurant le suivi, la coordination et le développement de la solution.

4.5.3 La main-d'œuvre :

La main-d'œuvre représente l'ensemble des ressources humaines nécessaires au développement, au déploiement et à la maintenance de la solution de télérelève sécurisée. Pour notre projet, les compétences requises sont les suivantes :

- **Ingénieurs en systèmes embarqués** : Chargés de la programmation et de la configuration des cartes ESP32, de l'extraction du CSI, de l'optimisation énergétique et de l'intégration du protocole MQTT.
- **Développeurs logiciels** : Responsables du développement de la plateforme de supervision, de la gestion des données de consommation, de l'API d'authentification et du tableau de bord de monitoring.
- **Spécialistes en cybersécurité** : Chargés de la conception et de la mise en œuvre des mécanismes d'authentification (challenge-réponse, cryptographie post-quantique), de la sécurisation des communications et des audits de vulnérabilités.
- **Ingénieurs réseau et intégration** : Responsables de l'intégration de la solution dans les infrastructures de communication existantes de Sonelgaz (SCADA, protocoles industriels), des tests sur le terrain et de la configuration réseau.
- **Chefs de projet** : Chargés de la coordination des activités, du suivi du projet, de la gestion des risques et de la relation avec les partenaires (Sonelgaz, universités, intégrateurs) et les clients.

L'entreprise compte employer au total 5 personnes à la première année, 12 personnes à la deuxième année, 14 personnes à la troisième année et 16 personnes à la quatrième année. Cet effectif change chaque année. On aura au total 20 personnes à la cinquième année de l'exercice. **Voici le tableau récapitulatif de l'effectif du personnel :**

TABLEAU RÉCAPITULATIF DE L'EFFECTIF DU PERSONNEL					
Projet AuthIoT-Sonelgaz					
Fonction	Année 1	Année 2	Année 3	Année 4	Année 5
Chef de projet / Directeur technique	1	1	1	1	1
Ingénieur cybersécurité IoT	1	2	2	3	3
Ingénieur systèmes embarqués IoT	1	3	4	5	6
Ingénieur réseau et intégration	0	1	1	1	2
Technicien IoT et maintenance	0	1	2	2	3
Responsable commercial B2B	0	1	1	1	1
Support technique et formation	0	1	1	1	2
Stagiaires / doctorants	2	2	2	2	2
Total	5	12	14	16	20

(a)

FIGURE 4.3 – Tableau récapitulatif de l'effectif du personnel

4.5.4 Les principaux partenaires :

Les partenaires constituent un élément stratégique pour le succès de notre projet. Ils apportent des compétences complémentaires, des ressources et un accès au marché que nous ne pourrions pas développer seuls. Nous avons identifié les partenaires clés suivants :

- **Sonelgaz** : Partenaire industriel potentiel et principal utilisateur de la solution pour la sécurisation des systèmes de télérelève des compteurs intelligents.
- **Université de Bouira** : Soutien scientifique et technique à travers l'encadrement académique et les activités de recherche.
- **Incubateur de l'Université de Bouira** : Accompagnement entrepreneurial, formation et soutien au développement du projet.
- **Fournisseurs de matériel électronique** : Approvisionnement en cartes ESP32, modules de communication et équipements nécessaires au déploiement de la solution.
- **Entreprises spécialisées en IoT et cybersécurité** apportent de l'expertise technique et des possibilités de collaboration pour l'intégration de la solution.
- **Organismes de soutien à l'innovation et aux startups** : Accompagnement, financement et mise en relation avec des partenaires industriels.

4.6 Cinquième axe : Plan financier

Le plan financier constitue un élément essentiel pour évaluer la faisabilité économique de notre projet LHAM, une solution logicielle de cybersécurité destinée à sécuriser les communications entre les compteurs intelligents et les systèmes centraux de gestion. Il permet d'estimer les coûts nécessaires à sa réalisation, les revenus potentiels attendus ainsi que les besoins financiers liés à son développement et à son déploiement. Cette analyse contribue à mesurer la rentabilité du projet et à assurer sa viabilité à long terme.

4.6.1 Les coûts et charges :

1. **Le total des coûts et charges :** Le tableau ci-dessous présente une projection globale de nos coûts et charges prévus sur les cinq prochaines années.

PRÉVISION Les Coûts - Investissements et Charges (En milliers DZD)					
Poste	N+1	N+2	N+3	N+4	N+5
PC (station développement)	300 000	240 000	180 000	120 000	60 000
PC (standard)	200 000	160 000	120 000	80 000	40 000
Bureau-Chaises-Armoire	150 000	120 000	90 000	60 000	30 000
Serveur d'application	500 000	400 000	300 000	200 000	100 000
Serveur de base de données	500 000	400 000	300 000	200 000	100 000
Serveur de communication	600 000	480 000	360 000	240 000	120 000
Switch réseau	80 000	64 000	48 000	32 000	16 000
Onduleur (UPS)	100 000	80 000	60 000	40 000	20 000
Équipement réseau	100 000	80 000	60 000	40 000	20 000
Outils de test et mesure	300 000	240 000	180 000	120 000	60 000
Total investissements	2 830 000	2 264 000	1 698 000	1 132 000	566 000
Réserves et provisions (10%)	283 000	226 400	169 800	113 200	56 600
Autres charges d'exploitation	1 930 000	2 660 000	3 420 000	4 170 000	4 920 000
Dépenses de personnel	340 000	1 040 000	1 240 000	1 460 000	1 890 000
Total général	5 383 000	6 190 400	6 527 800	6 875 200	7 432 600

(a)

FIGURE 4.4 – Les coûts.

2. **Immobilisation corporelles :** Amortissement des biens matériels sur 5 ans selon un taux linéaire de 20

IMMOBILISATIONS CORPORELLES Amortissement linéaire sur 5 ans (taux 20%)					
(En milliers DZD)					
Immobilisation	N+1	N+2	N+3	N+4	N+5
Switch réseau	80 000	64 000	48 000	32 000	16 000
Serveur d'application	500 000	400 000	300 000	200 000	100 000
Serveur de base de données	500 000	400 000	300 000	200 000	100 000
Serveur de communication (modems GSM)	600 000	480 000	360 000	240 000	120 000
Onduleur (UPS)	100 000	80 000	60 000	40 000	20 000
PC station développement	300 000	240 000	180 000	120 000	60 000
PC standard	200 000	160 000	120 000	80 000	40 000
Bureau, chaises et armoire	150 000	120 000	90 000	60 000	30 000
Équipement réseau (câbles, connectique)	100 000	80 000	60 000	40 000	20 000
Outils de test et mesure	300 000	240 000	180 000	120 000	60 000
TOTAL IMMOBILISATION NETTE	2 830 000	2 264 000	1 698 000	1 132 000	566 000

(a)

FIGURE 4.5 – Immobilisation corporelle.

3. **Autres charges d'exploitation** : loyer et charges locatives, déplacements et frais de mission (suivi pilote Sonelgaz), marketing et communication, hébergement cloud et serveurs, certification et audit sécurité, frais juridiques et comptables, fournitures et matériel de bureau, maintenance matérielle.

AUTRES CHARGES D'EXPLOITATION

(En milliers DZD)

Poste	N-2	N-1	N	N+1	N+2	N+3	N+4	N+5
Loyer et charges locatives	/	/	/	480 000	600 000	720 000	840 000	960 000
Déplacements et frais de mission (Sonelgaz)	/	/	/	360 000	480 000	600 000	720 000	840 000
Marketing et communication	/	/	/	240 000	360 000	480 000	600 000	720 000
Hébergement cloud et serveurs	/	/	/	300 000	420 000	540 000	660 000	780 000
Certification et audit sécurité	/	/	/	200 000	300 000	400 000	500 000	600 000
Frais juridiques et comptables	/	/	/	120 000	180 000	240 000	300 000	360 000
Fournitures et matériel de bureau	/	/	/	80 000	120 000	160 000	200 000	240 000
Maintenance matérielle	/	/	/	150 000	200 000	280 000	350 000	420 000
TOTAL AUTRES CHARGES D'EXPLOITATION	/	/	/	1 930 000	2 660 000	3 420 000	4 170 000	4 920 000

(a)

FIGURE 4.6 – Autres charges d'exploitation

4. **Dépenses de personnel** : masse salariale incluant salaires et charges sociales (40 %), avec une équipe passant de 5 à 20 personnes sur 5 ans, évoluant de manière
5. **progressive** : 5 (N+1), 12 (N+2), 14 (N+3), 16 (N+4) et 20 (N+5).

PLAN DE RECRUTEMENT ET MASSE SALARIALE (Évolution prévisionnelle des effectifs et des coûts salariaux sur 5 ans) (En milliers DZD)					
Poste	N+1	N+2	N+3	N+4	N+5
Ingénieur cybersécurité IoT	80 000	100 000	120 000	120 000	150 000
Chef de projet	120 000	240 000	240 000	360 000	360 000
Développeur	100 000	300 000	400 000	500 000	600 000
Ingénieur réseau	0	100 000	100 000	100 000	200 000
Technicien maintenance	0	80 000	160 000	160 000	240 000
Responsable commercial	0	100 000	100 000	100 000	100 000
Support technique	0	80 000	80 000	80 000	200 000
Stagiaires / doctorants	40 000	40 000	40 000	40 000	40 000
TOTAL MASSE SALARIALE	340 000	1 040 000	1 240 000	1 460 000	1 890 000

FIGURE 4.7 – Les dépenses de personnel

6. **Modalités et sources d’approvisionnement** : Le projet est financé grâce à la participation de l’équipe des fondateurs, possédant notamment une expérience suffisante dans le domaine de la cybersécurité, des systèmes embarqués et de la télérelève des compteurs intelligents.

Comment récupérer de l’argent : cela se fait grâce aux revenus de la première année de travail (N+1), qui s’élèvent à 8,64 millions de DZD, couvrant largement les coûts opérationnels de 4,88 millions de DZD et générant un gain de 3,76 millions de DZD — avec une progression prévisionnelle atteignant 93,88 millions de DZD de revenus à N+5.

Les coûts et Revenus									
(En milliers DZD)									
Num	Poste	N-2	N-1	N	N+1	N+2	N+3	N+4	N+5
1	Revenus	/	/	/	8 640 000	17 100 000	28 960 000	52 120 000	93 880 000
2	Coûts	/	/	/	5 383 000	6 190 400	6 527 800	6 875 200	7 432 600
3	Gains	/	/	/	3 257 000	10 909 600	22 432 200	45 244 800	86 447 400

FIGURE 4.8 – Les coûts et revenus.

4.6.2 Chiffre d'affaires :

Les revenus de notre solution de télérelève sécurisée proviennent de plusieurs services, notamment :

- **Service principal A** : Vente et déploiement de la solution de télérelève sécurisée.
- **Service principal B** : Installation et configuration des équipements (modules de communication et plateforme).
- **Service principal C** : Maintenance, assistance technique et mises à jour de sécurité.
- **Service principal D** : Formation et accompagnement des utilisateurs et opérateurs.

Tableau de chiffre d'affaires pessimiste : Le tableau ci-dessous illustre nos prévisions de ventes sur une période de cinq ans en milliers de DZD , adoptant une perspective pessimiste.

DETAIL DU CHIFFRE D'AFFAIRES - SCENARIO PESSIMISTE

Service	Unités	Prix unitaires (DZD)	N+1	N+2	N+3	N+4	N+5
Vente solution	Licences	1 000 000	4 500 000	9 000 000	14 000 000	20 000 000	27 000 000
Installation	Sites installés	400 000	400 000	700 000	1 000 000	1 300 000	1 600 000
Maintenance	Contrats	300 000	300 000	600 000	900 000	1 200 000	1 500 000
Formation	Sessions	100 000	100 000	200 000	300 000	400 000	500 000
CHIFFRE D'AFFAIRES GLOBAL			5 300 000	10 500 000	16 200 000	22 900 000	30 600 000

FIGURE 4.9 – Pessimisme des ventes.

Chiffre d'affaires optimiste : le tableau ci-dessous illustre nos prévisions optimistes concernant les ventes sur cinq ans en milliers de DZD.

DETAIL DU CHIFFRE D'AFFAIRES - SCENARIO OPTIMISTE

Service	Unités	Prix unitaires (DZD)	N+1	N+2	N+3	N+4	N+5
Vente solution	Licences	1 000 000	7 000 000	14 000 000	23 000 000	34 000 000	45 000 000
Installation	Sites installés	400 000	800 000	1 400 000	2 000 000	2 500 000	3 000 000
Maintenance	Contrats	300 000	600 000	1 200 000	2 000 000	3 000 000	4 500 000
Formation	Sessions	100 000	200 000	500 000	800 000	1 200 000	1 800 000
CHIFFRE D'AFFAIRES GLOBAL			8 600 000	17 100 000	27 800 000	40 700 000	54 300 000

FIGURE 4.10 – Optimisme des ventes.

4.7 Les comptes de résultat attendus :

Le compte de résultat prévisionnel permet d'évaluer la rentabilité future du projet en comparant les revenus attendus aux charges prévues.

1. Méthode de calcul :

- **Consommation de l'exercice** : achats de matériel + services extérieurs + frais de communication + frais d'hébergement + autres charges d'exploitation.
- **Valeur ajoutée d'exploitation** : Chiffre d'affaires $\sim$ consommation de l'exercice.
- **Excédent brut d'exploitation** : valeur ajoutée d'exploitation $\sim$ dépenses de personnel.
- **Résultat ordinaire avant impôt** : excédent brut d'exploitation $\sim$ dotations aux amortissements.

L'analyse de ces indicateurs permet d'estimer la capacité du projet à générer des bénéfices et à assurer son développement à long terme.

1. **Besoin en fonds de roulement** : Le BFR représente les ressources financières nécessaires pour couvrir les dépenses courantes du projet avant l'encaissement des revenus.
2. **BFR = Actifs circulants – Passifs circulants** : Dans notre projet, les actifs circulants comprennent principalement la trésorerie disponible, les créances clients et les stocks éventuels de matériel. Les passifs circulants correspondent aux dettes à court terme et aux charges à payer.
3. **Fonds de roulement** : Le FR représente les ressources financières stables dont dispose le projet pour financer son activité.
4. **FR = Capitaux permanents – Actifs immobilisés** : Les capitaux permanents comprennent les apports des fondateurs, les aides financières et les subventions éventuelles. Les actifs immobilisés regroupent les équipements informatiques et les autres matériels utilisés pour le projet.
5. **Plan de trésorerie** : La trésorerie correspond aux liquidités disponibles permettant d'assurer le fonctionnement quotidien du projet. **Trésorerie** (: $FR \sim BFR$

Une trésorerie positive garantit la capacité du projet à faire face à ses dépenses courantes et à financer son développement future.

FR	5 695 167
BFR	813 567
TR	4 881 600

TABLE 4.2 – Calculer les besoins en capital de Monarch

4.8 Sixième axe : Prototype expérimental

4.8.1 Environnements de développement :

1. Outils de rédaction

LaTeX :

LaTeX est un système de composition de documents libre et open source, largement utilisé pour la rédaction de documents scientifiques et techniques grâce à sa qualité typographique et à ses puissantes fonctionnalités de mise en page.

Site officiel :

- <https://www.latex-project.org/>
- <https://www.latex-project.org/about/> (consulté le 22 juin 2026).

Nous avons choisi LaTeX plutôt qu'un logiciel de traitement de texte classique, tel que Microsoft Word ou OpenOffice, pour les raisons suivantes :

- Il est gratuit et open source.
- Il offre une mise en page professionnelle et de haute qualité.
- Il est particulièrement adapté à la rédaction de documents scientifiques et techniques.
- Il facilite la gestion automatique des références bibliographiques, des figures, des tableaux et de la table des matières.
- Il utilise un système de commandes permettant une organisation claire du document et une présentation homogène.

2. Outils de Programmation : Arduino :

C'est une plateforme open source de prototypage électronique basée sur des cartes programmables et un IDE. Elle permet de concevoir facilement des systèmes embarqués et des projets IoT en combinant matériel et logiciel. **Site officiel :**

— <https://www.arduino.cc/en/Guide/Introduction>

Visual Studio Code :

VS Code est un éditeur de code source gratuit développé par Microsoft. Il offre un environnement de développement flexible permettant la création, l'édition et le débogage de programmes dans plusieurs langages de programmation.

— <https://code.visualstudio.com>

3. Langages de Programmation :

C/C++ est un langage de programmation utilisé pour développer des applications performantes, notamment dans les systèmes embarqués, les microcontrôleurs et les objets connectés.

— <https://www.cplusplus.com/doc/tutorial/>

Pourquoi C/C++ ?

- Performant et rapide à exécuter.
- Adapté aux systèmes embarqués et aux objets IoT.
- Compatible avec l'ESP32 et Arduino IDE.
- Faible consommation des ressources matérielles.
- Permet un contrôle direct du matériel.

4.8.2 Implémentation de la base de données

La plateforme de supervision utilise une base de données SQLite intégrée, choisie pour sa légèreté et sa simplicité de déploiement. Contrairement aux systèmes de gestion de base de données client-serveur (MySQL, PostgreSQL), SQLite ne nécessite aucun processus serveur séparé ni configuration réseau complexe, ce qui la rend particulièrement adaptée au contexte du prototype.

Structure de la base de données : Le schéma relationnel comprend trois tables principales :

- **compteurs** : stocke les informations d'identification des compteurs intelligents (identifiant, PDL, clé secrète partagée, adresse IP, statut de connexion).
- **releves** : enregistre l'historique des télérelevés (date, index de consommation, consommation incrémentale, nonce utilisé, type de relève).

- **authentications** : journalise les tentatives d'authentification (horodatage, résultat, hash de vérification) pour la traçabilité et l'audit de sécurité.

Technologies utilisées : L'accès à la base de données est assuré par l'ORM SQLAlchemy sous Python, via l'environnement de développement VC Code. Cette approche permet une abstraction efficace des opérations CRUD (Create, Read, Update, Delete) et garantit la portabilité du code entre différents environnements de test.

4.8.3 Interface de Programmation

L'interface de programmation du système se décompose en deux parties complémentaires : le **firmware embarqué** exécuté sur l'ESP32 (côté compteur intelligent) et l'**API REST** déployée sur la plateforme de supervision (côté serveur). Cette dualité assure une communication structurée et sécurisée entre les entités du protocole.

1. **Interface de programmation côté Arduino (ESP32)** : Le firmware de compteur intelligent est développé en C/C++ sous Arduino IDE et implémente l'ensemble des mécanismes cryptographiques et de communication du protocole. Le démarrage du système suit une séquence d'initialisation rigoureuse, illustrée par les figures 4.11 , 4.12 et 4.13.

```

-----
[001] WiFi OK: 192.168.1.101
[001] mDNS: smart-meter-001.local
[001] OTA ready
[001] Test connexion vers 192.168.1.9:5000
[001] CONNEXION PLATEFORME OK !
[001] Telegram: 🚀 <b>SMART METER 001 démarré</b> %OAIP: 192.16
[001] Prêt
Device: SMART_METER_001
Client: Client Industriel Alpha
Ref: REF-ALPHA-2024
Index: 6563322.50 kWh
MAC: 88:F1:55:31:4E:54
❤️ [001] Heartbeat OK (IP: 192.168.1.101)
🇮🇹 [001] SMART_METER_001 | Index: 6563322.50 kWh

```

FIGURE 4.11 – Séquence de démarrage du compteur intelligent 001 — Connexion WiFi, mDNS, OTA, plateforme et Telegram

```
.....
[002] WiFi OK: 192.168.1.103
[002] mDNS: smart-meter-002.local
[002] OTA ready
[002] Test connexion vers 192.168.1.9:5000
[002] CONNEXION PLATEFORME OK !
[002] Telegram: 🚀 <b>SMART METER 002 démarré</b>%0AIP: 192.16
[002] Prêt
Device: SMART_METER_002
Client: Client Industriel Beta
Ref: REF-BETA-2024
Index: 10004461.00 kWh
MAC: 8C:94:DF:4C:2D:0C
❤️ [002] Heartbeat OK (IP: 192.168.1.103)
📊 [002] SMART_METER_002 | Index: 10004461.00 kWh
```

FIGURE 4.12 – Séquence de démarrage du compteur intelligent 002 — Vérification de la chaîne de connexion complète

```
[003] WiFi OK: 10.61.204.132
[003] mDNS: smart-meter-003.local
[003] OTA ready
[003] Test connexion vers 10.61.204.112:5000
[003] CONNEXION PLATEFORME OK !
[003] Telegram: 🚀 <b>SMART METER 003 démarré</b>%0AIP: 10.61.
[003] Prêt
Device: SMART_METER_003
Client: Client Industriel Gamma
Ref: REF-GAMMA-2024
Index: 8429075.00 kWh
MAC: 8C:94:DF:4C:2D:0C
❤️ [003] Heartbeat OK (IP: 10.61.204.132)
📊 [003] SMART_METER_003 | Index: 8429075.00 kWh
```

FIGURE 4.13 – Séquence de démarrage du compteur intelligent 003 — Vérification de la chaîne de connexion complète

2. **Interface de supervision (Dashboard)** : La plateforme de supervision a été développée avec le framework Flask et offre une interface web intuitive permettant de visualiser l'état des compteurs intelligents en temps réel. L'interface principale présente une vue d'ensemble de l'ensemble du parc de compteurs (figure 4.14).

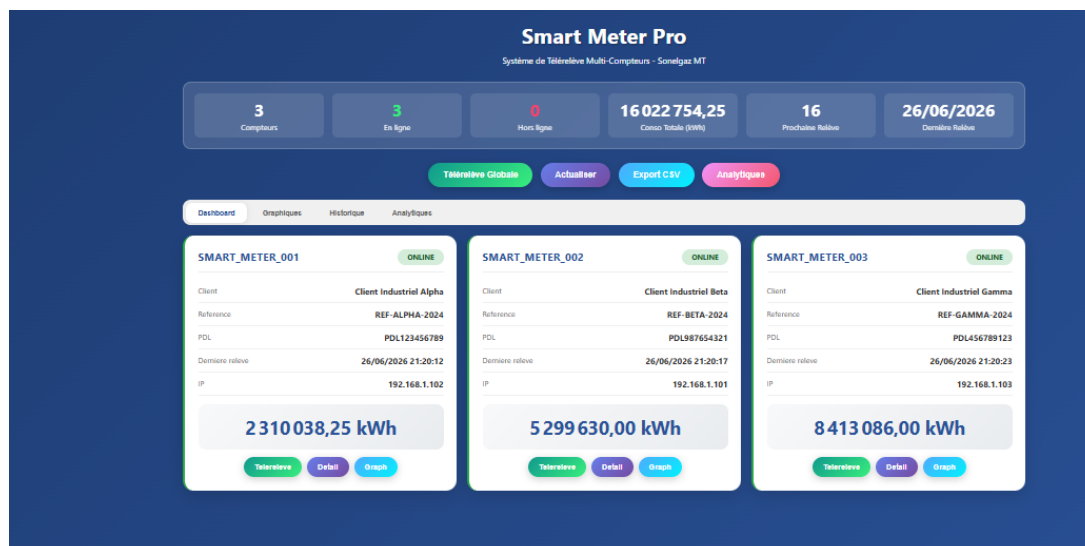


FIGURE 4.14 – Vue d'ensemble du dashboard de supervision

Chaque compteur est représenté par une carte affichant son identifiant, son statut de connexion (en ligne/hors ligne), l'index de consommation actuel et le PDL associé (figure 4.15).

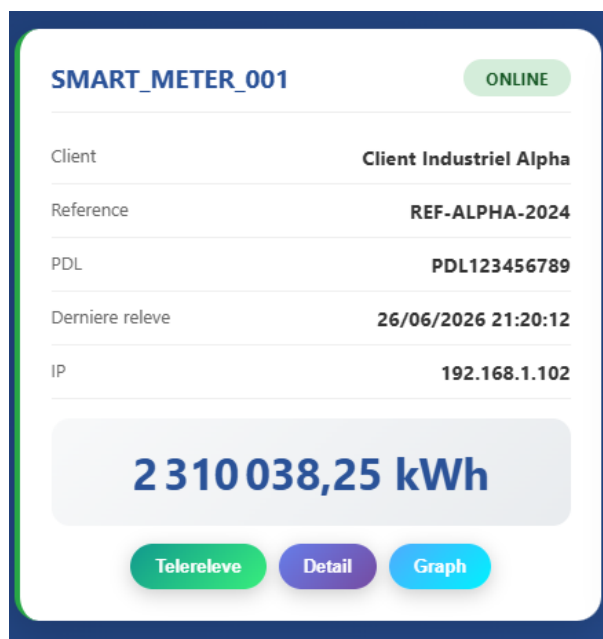


FIGURE 4.15 – Détail d'un compteur sur le dashboard

L'opérateur peut initier une télérelève en cliquant sur le bouton « Télérelève ». Une fenêtre modale apparaît alors pour la saisie de l'OTP reçu via Telegram (figure 4.16).



FIGURE 4.16 – Fenêtre de saisie de l’OTP

Après validation, le résultat de la télérelève est affiché avec l’index, l’incrément de consommation, le nonce utilisé et le hash d’authentification (figure 4.17).

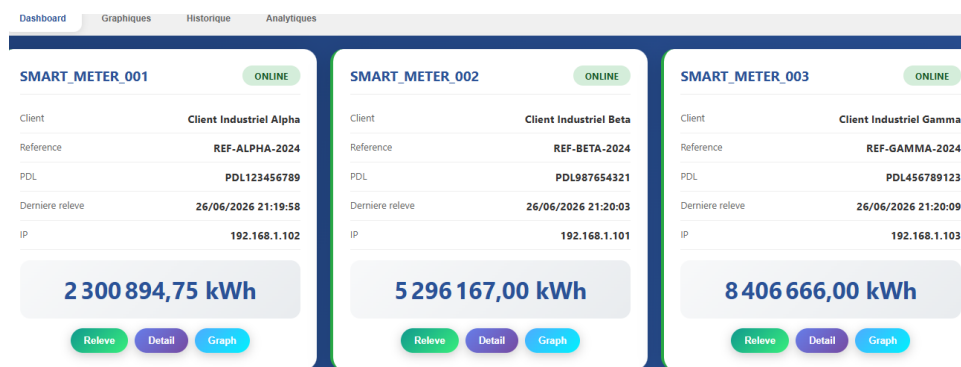


FIGURE 4.17 – Résultat d’une télérelevé réussie

Visualisation graphique des données :

L’interface intègre une section dédiée aux graphiques analytiques permettant de visualiser l’évolution de la consommation énergétique au fil du temps. Plusieurs types de graphiques sont disponibles : la courbe d’index cumulé, l’histogramme des consommations par relevé, le comparatif mensuel ainsi que la répartition entre relèves manuels et programmés (figure 4.18).

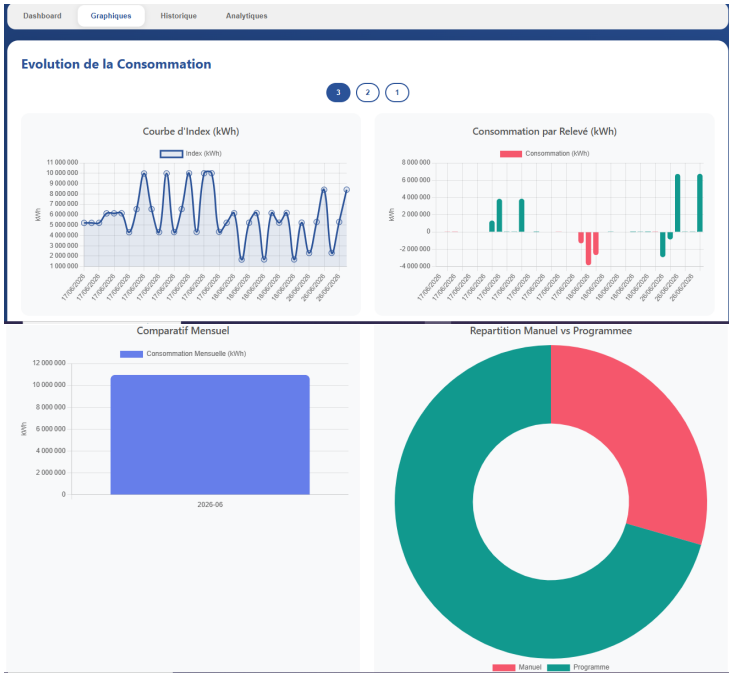


FIGURE 4.18 – Graphiques analytiques de consommation

3. Historique des relèves

Une section historique permet de consulter l’ensemble des relevés effectués, présentés sous forme de tableau chronologique (figure 4.19). Chaque entrée indique la date de la relève, l’identifiant du compteur, le client associé, l’index enregistré, la consommation incrémentale, le nonce de sécurité utilisé ainsi que le type de relève (manuelle ou programmée).

Historique des Relevés						
Tous les compteurs			Exporter			
Date	Compteur	Client	Index (kWh)	Conso (kWh)	Nonce	Type
26/06/2026 21:20:23	--	Client Industriel Gamma	8 413 086,00	+6734 306,37	globa1...	Programme
26/06/2026 21:20:17	--	Client Industriel Beta	5 299 630,00	+3463,00	globa1...	Programme
26/06/2026 21:20:12	--	Client Industriel Alpha	2 310 038,25	+9 143,50	globa1...	Programme
26/06/2026 21:20:09	--	Client Industriel Gamma	8 406 666,00	+6727 886,37	globa1...	Programme
26/06/2026 21:20:03	--	Client Industriel Beta	5 296 167,00	+870 190,00	globa1...	Programme
26/06/2026 21:19:58	--	Client Industriel Alpha	2 300 894,75	+2 929 811,75	globa1...	Programme
26/06/2026 20:26:22	--	Client Industriel Alpha	5 230 706,50	+4 346,00	94dd234a...	Manuel

FIGURE 4.19 – Tableau d’historique des relèves

4. Export des données

La plateforme offre la possibilité d’exporter l’ensemble des données de consommation au format CSV, facilitant ainsi leur exploitation externe ou leur archivage. L’ex-

port peut être global (tous les compteurs) ou ciblé sur un compteur spécifique via l'historique (figure 4.20).

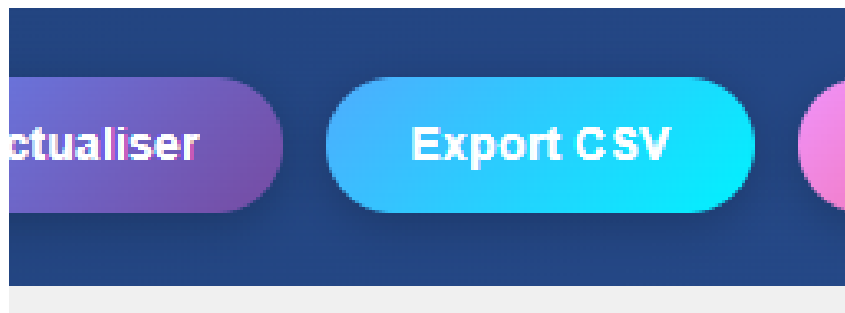


FIGURE 4.20 – Interface d'export des données en CSV

Le fichier CSV généré (figure 4.21) contient les champs suivants : date de la télérelève, identifiant du compteur, nom du client, PDL, index enregistré, consommation incrémentale et type de relève (manuelle ou programmée). Ce format standard permet une intégration aisée avec des outils de tableur ou des systèmes de facturation externes.

1	Date,Compteur,Client,PDL,Index,Conso,Type
2	2026-06-26T21:20:12.638141,SMART_METER_001,Client Industriel Alpha,PDL123456789,2310038.25,9143.5,Programme
3	2026-06-26T21:19:58.393972,SMART_METER_001,Client Industriel Alpha,PDL123456789,2300894.75,-2929811.75,Programme
4	2026-06-26T20:26:22.391346,SMART_METER_001,Client Industriel Alpha,PDL123456789,5230706.5,4346.0,Manuel
5	2026-06-18T14:11:52.118790,SMART_METER_001,Client Industriel Alpha,PDL123456789,5226360.5,2077.0,Programme
6	2026-06-18T10:48:50.514373,SMART_METER_001,Client Industriel Alpha,PDL123456789,5224283.5,4887.5,Programme
7	2026-06-18T10:14:06.848138,SMART_METER_001,Client Industriel Alpha,PDL123456789,5219396.0,-1320809.5,Manuel
8	2026-06-17T18:26:15.349907,SMART_METER_001,Client Industriel Alpha,PDL123456789,6540205.5,1838.5,Programme
9	2026-06-17T18:24:51.271368,SMART_METER_001,Client Industriel Alpha,PDL123456789,6538367.0,6819.0,Programme
10	2026-06-17T18:24:43.719034,SMART_METER_001,Client Industriel Alpha,PDL123456789,6531548.0,1320687.5,Programme
11	2026-06-17T17:34:01.242564,SMART_METER_001,Client Industriel Alpha,PDL123456789,5210860.5,3796.5,Manuel
12	2026-06-17T17:32:31.587944,SMART_METER_001,Client Industriel Alpha,PDL123456789,5207064.0,2269.5,Manuel
13	2026-06-17T17:32:23.537031,SMART_METER_001,Client Industriel Alpha,PDL123456789,5204794.5,0.0,Manuel
14	2026-06-26T21:20:17.856941,SMART_METER_002,Client Industriel Beta,PDL987654321,5299630.0,3463.0,Programme
15	2026-06-26T21:20:03.759291,SMART_METER_002,Client Industriel Beta,PDL987654321,5296167.0,-870190.0,Programme
16	2026-06-18T14:11:57.497558,SMART_METER_002,Client Industriel Beta,PDL987654321,6166357.0,7076.5,Programme
17	2026-06-18T11:06:43.659339,SMART_METER_002,Client Industriel Beta,PDL987654321,6159280.5,7859.5,Manuel
18	2026-06-18T10:48:56.694557,SMART_METER_002,Client Industriel Beta,PDL987654321,6151421.0,10728.0,Programme
19	2026-06-18T10:42:07.620294,SMART_METER_002,Client Industriel Beta,PDL987654321,6140693.0,-3863768.0,Manuel
20	2026-06-17T20:05:19.827267,SMART_METER_002,Client Industriel Beta,PDL987654321,10004461.0,5777.0,Programme
21	2026-06-17T19:38:34.630779,SMART_METER_002,Client Industriel Beta,PDL987654321,9998684.0,3810.0,Manuel

FIGURE 4.21 – Contenu d'un fichier CSV exporté

- 5. Notifications Telegram :** Le service Telegram est utilisé comme canal sécurisé pour la transmission du second facteur d'authentification. Lorsqu'une demande de télérelève est initiée, le compteur intelligent génère un code OTP à usage unique et l'envoi directement au client via le bot Telegram (figure 4.22,4.23).

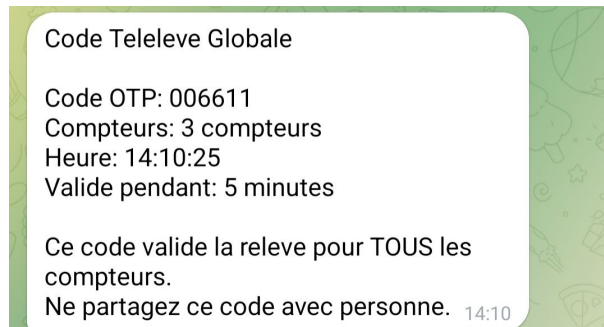


FIGURE 4.22 – Notification OTP reçue sur Telegram



FIGURE 4.23 – Notification OTP reçue sur Telegram

Une fois la téléreleve effectuée et validée, une notification de confirmation est envoyée, incluant l'index de consommation, l'incrément, le nonce et le hash d'authentification (figure 4.24, 4.25).

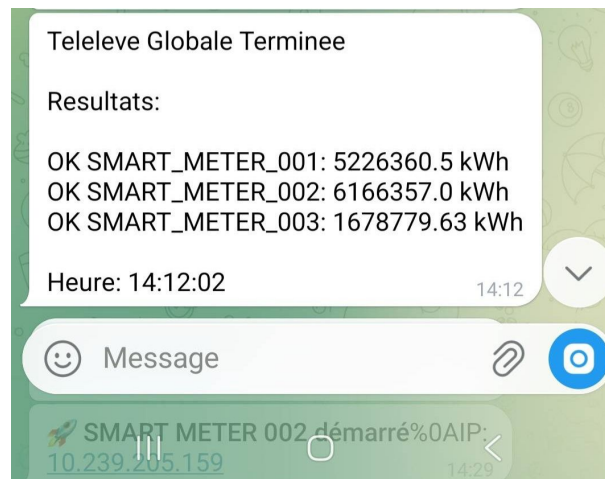


FIGURE 4.24 – Confirmation de télérelevé avec preuve d'authentification

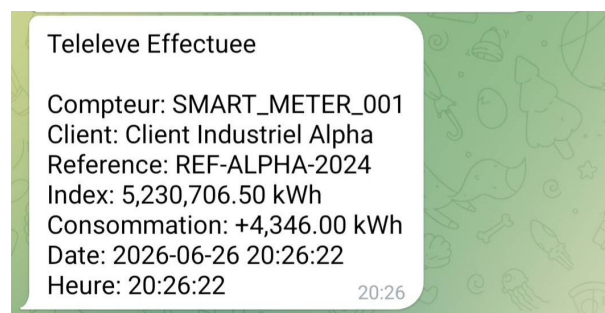


FIGURE 4.25 – Confirmation de télérelevé avec preuve d'authentification

Le système assure également la supervision des équipements grâce aux alertes de déconnexion et de reconnexion.(figure 4.26)



FIGURE 4.26 – Alerte de déconnexion d'un compteur

4.9 Conclusion

Au terme de ce chapitre, nous avons présenté l'étude technico-économique et financière du projet afin d'évaluer sa faisabilité dans un contexte réel de déploiement. Les différentes analyses réalisées, notamment l'étude du marché, le plan de production et d'organisation, le plan de recrutement ainsi que les prévisions financières, ont permis de mettre en évidence le potentiel de développement de la solution proposée.

Les résultats obtenus montrent que le projet repose sur un modèle économique cohérent et présente des perspectives de rentabilité encourageantes. Ainsi, cette étude confirme que la solution proposée est non seulement pertinente sur le plan technique, mais également viable sur les plans économique et organisationnel, ce qui constitue un atout pour son développement et son éventuel déploiement à plus grande échelle.

Conclusion et Perspectives

L'IoT occupe aujourd'hui une place importante dans de nombreux domaines, notamment les réseaux intelligents. Toutefois, la sécurisation des communications entre les objets connectés demeure un défi majeur en raison de leurs ressources limitées. Dans ce contexte, le développement de protocoles d'authentification légers constitue une solution essentielle pour garantir des échanges fiables et sécurisés.

Dans ce mémoire, nous avons proposé un protocole d'authentification léger destiné aux compteurs intelligents (les entreprises énergétiques, les industries utilisent les systèmes de télérelève). Notre solution repose sur une authentification mutuelle utilisant des fonctions de hachage, des nonces et un code OTP transmis via un service de messagerie sécurisé (Telegram dans notre prototype), afin de renforcer la sécurité des échanges entre le compteur intelligent et la plateforme de supervision.

Afin de valider cette proposition, une implémentation expérimentale a été réalisée à l'aide d'une carte ESP32, d'une plateforme développée sous VS Code et d'une base de données. Les tests effectués ont montré le bon fonctionnement du protocole ainsi que sa capacité à résister aux principales attaques, notamment les attaques par rejeu, l'usurpation d'identité et l'interception des communications.

Par ailleurs, une étude technico-économique a permis d'évaluer la faisabilité du projet à travers l'élaboration d'un BMC, de prévisions financières et d'une analyse de rentabilité. Les résultats obtenus montrent que notre solution est non seulement techniquement réalisable, mais également économiquement cohérente.

Comme toute étude, ce travail présente certaines limites, notamment le fait que les

expérimentations ont été réalisées dans un environnement de test. Un déploiement sur une infrastructure réelle permettrait d'évaluer davantage les performances du protocole dans des conditions d'exploitation réelles.

Comme perspectives, il serait intéressant de tester le protocole sur un réseau de plus grande envergure, d'intégrer un mécanisme de gestion dynamique des clés cryptographiques et de remplacer le service Telegram par une solution OTP professionnelle directement intégrée à la plateforme. L'intégration du protocole avec des plateformes Cloud IoT industrielles constitue également une perspective prometteuse.

En définitive, ce travail nous a permis de concevoir, d'implémenter et d'évaluer une solution d'authentification légère adaptée aux contraintes des systèmes IoT. Nous espérons que cette contribution pourra servir de base à de futurs travaux visant à renforcer la sécurité des objets connectés et des infrastructures de comptage intelligent.

Bibliographie

- [1] Introduction. <https://www.sentinelone.com/fr/cybersecurity-101/data-and-ai/iot-security-risks/>.
- [2] Définition. <https://dspace.ummto.dz/server/api/core/bitstreams/b6a36127-f4db-4d01-8f86-6468e931c763/content>.
- [3] Historique. https://rivieresdusud.uaszh.sn/bitstream/handle/123456789/1378/sow_memoire_2021.pdf.
- [4] Architecture. <https://hal.science/hal-03593723/>.
- [5] Contrainte d'énergie 1. <https://ds.univ-oran2.dz:8443/jspui/bitstream/123456789/7744/1/ZK%20MFE%20MAII.pdf>.
- [6] Contrainte d'énergie 2. <https://ressi2025.sciencesconf.org/615408/document>.
- [7] Contraintes de calcul. <https://eduscol.education.gouv.fr/sites/default/files/document/ra19lyceegtsispecoursiot1207080pdf-82107.pdf>.
- [8] Contraintes de mémoire. https://learninglab.gitlabpages.inria.fr/mooc-iot/mooc-iot-ressources/Module4/S01/C034AA-M04-S01-part1cours_FR.html.
- [9] Sécurité dans l'IoT. <https://fr.scribd.com/document/689356026/Definition-de-la-Securite-de-l>.
- [10] Sécurité des données. <https://nexus.ingroupe.com/fr/securite-iot-definition/>.
- [11] Sécurité des dispositifs. <https://dspace.univ-oran1.dz/items/f998de95-31df-44c6-9c9b-4cbc9713219f>.

- [12] Sécurité des communications. <https://www.ass-security.fr/blog/protocole-mqtt-iot-objets-connectes-cyberattaque/>.
- [13] Confidentialité. <https://canadafr.neotrust.io/post/les-3-principes-de-la-securite-de-l-information/>.
- [14] Intégrité. <https://www.sentinelone.com/fr/cybersecurity-101/cybersecurity/cyber-security-principles/>.
- [15] Disponibilité. <https://www.box.com/fr-fr/resources/what-is-information-security>.
- [16] Authenticité. <https://cursa.app/fr/page/principes-de-securite-de-l-information>.
- [17] Non-répudiation. <https://cursa.app/fr/page/principes-de-securite-de-l-information>.
- [18] Menaces. <https://fr.vectra.ai/topics/iot-security>.
- [19] Attaque par jeu. <https://fr.vectra.ai/topics/iot-security>.
- [20] Usurpation d'identité. https://docs.aws.amazon.com/fr_fr/iot-device-defender/latest/devguide/dd-detect-security-use-cases.html.
- [21] Attaque homme-du-milieu (MITM). <https://www.fortinet.com/fr/resources/cyberglossary/man-in-the-middle-attack>.
- [22] Interception. https://www.murielle-cahen.com/publications/p_interception_donnees.asp.
- [23] Contraintes matérielles. <https://www.seidor.com/fr-dz/blog/securite-iot-defis-strategies>.
- [24] Contraintes d'authentification. <https://clusir.corsica/la-securite-des-iot-internet-des-objets-defis-et-solutions/>.
- [25] Contraintes organisationnelles. <https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/cybersecurite-attaques-et-mesures-de-protection-des-si-42313210/risques-en-cybersecurite-de-l-iot-h5846/>.
- [26] Cryptographie légère. <https://www.silicon.fr/Thematique/cybersecurite-1371/Breves/nist-normalise-cryptographie-legere-iot-484953.htm>.

- [27] Cryptographie légère : chiffrement. <https://fr.scribd.com/document/666740857/TPE-CRYPTO-LEGERE-1>.
- [28] Protocoles d'authentification. <https://www.keyfactor.com/fr/blog/the-top-iot-authentication-methods-and-options/>.
- [29] Protocoles d'authentification : hash. https://fr.wikipedia.org/wiki/Signature_de_Lamport.
- [30] Gestion des clés dynamiques. <https://www.keyfactor.com/fr/blog/best-practices-for-public-key-vs-private-key-management/>.
- [31] Renouvellement des clés. https://fr.wikipedia.org/wiki/Signature_de_Lamport.
- [32] Introduction chapitre 2. <https://www.keyfactor.com/fr/blog/the-top-iot-authentication-methods-and-options/>.
- [33] Importance de l'authentification. <https://www.keyfactor.com/fr/blog/the-top-iot-authentication-methods-and-options/>.
- [34] Définition de l'authentification. <https://www.lemagit.fr/definition/Authentification>.
- [35] Authentification vs Autorisation. <https://www.fortinet.com/fr/resources/cyberglossary/authentication-vs-authorization>.
- [36] Authentification unilatérale. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074647/authentication-unidirectionnelle>.
- [37] Authentification mutuelle. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074646/authentication-mutuelle>.
- [38] Tableau comparatif. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074647/authentication-unidirectionnelle>.
- [39] Authentification par mot de passe. <https://www.php.net/manual/fr/function.password-hash.php>.
- [40] Fonctions de hachage. https://learninglab.gitlabpages.inria.fr/mooc-iot/mooc-iot-ressources/Module6/S02/C034AA-M06-S02-cours-part2_FR.html.
- [41] Challenge-Response. <https://jumpcloud.com/it-index/what-is-challenge-response-authentication>.

- [42] Exemples. https://fr.wikipedia.org/wiki/Signature_de_Lamport.
- [43] Consommation élevée. <https://www.veonum.com/ecosysteme-esp32-guide-developpeurs-iot/>.
- [44] Complexité. <https://www.globalsign.com/fr/blog/securite-iot-pki-relevez-le-defis>.
- [45] Gestion des clés. <https://www.certeurope.fr/blog/pki-iot/>.
- [46] Définition du Smart Meter. <https://www.deepki.com/fr/glossaire/smart-meter/>.
- [47] Smart Meter. <https://dspace.ummto.dz/server/api/core/bitstreams/0f580687-555c-47a8-877e-24aff41311b8/content>.
- [48] Auteur inconnu. Contraintes matérielles critiques, 2024. Document PDF local.
- [49] Profil des compteurs. Catalogue Sonelgaz 2024 — document local PDF.
- [50] Profil des compteurs. <https://dspace.univ-tiaret.dz/server/api/core/bitstreams/952b5cba-fa19-45ce-a3a4-0b9e6ee30091/content>.
- [51] Tableau comparatif 2. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074646/authentication-mutuelle>.

Annexe A

Annexe A

ACTIF								
(En milliers DZD)								
En milliers DZD	REALISATION			PREVISION				
	N-2	N-1	N	N+1	N+2	N+3	N+4	N+5
• Immobilisation Incorporelles	/	/	/	200 000	180 000	160 000	140 000	120 000
• Immobilisation Corporelles	/	/	/	2 830 000	2 264 000	1 698 000	1 132 000	566 000
Terrain	/	/	/	/	/	/	/	/
Bâtiment	/	/	/	/	/	/	/	/
Autres Immobilisations Corporelles	/	/	/	/	/	/	/	/
Immobilisations en concession	/	/	/	/	/	/	/	/
Immobilisation en cours	/	/	/	/	/	/	/	/
Immobilisations Financières	/	/	/	/	/	/	/	/
Titres mis en équivalence	/	/	/	/	/	/	/	/
Autres participations et créances rattachées	/	/	/	/	/	/	/	/
Autres Titres immobilisés	/	/	/	/	/	/	/	/
Prêts et autres titres financiers non courants	/	/	/	/	/	/	/	/
Impôts différés actif	/	/	/	/	/	/	/	/
ACTIF NON COURANT	/	/	/	3 030 000	2 444 000	1 858 000	1 272 000	686 000
Stocks et encours	/	/	/	500 000	700 000	1 000 000	1 300 000	1 600 000
Créances et emplois assimilés	/	/	/	1 000 000	1 800 000	2 800 000	4 500 000	7 000 000
Clients	/	/	/	1 000 000	1 800 000	2 800 000	4 500 000	7 000 000
Autres débiteurs	/	/	/	/	/	/	/	/
Impôts et assimilés	/	/	/	/	/	/	/	/
Autres créances et emplois assimilés	/	/	/	/	/	/	/	/
• Disponibilités et assimilés	/	/	/	1 500 000	4 000 000	8 000 000	15 000 000	28 000 000
Placements et autres actifs financiers courants	/	/	/	0	0	500 000	1 000 000	2 000 000
Trésorerie	/	/	/	1 500 000	4 000 000	8 000 000	15 000 000	28 000 000
ACTIF COURANT	/	/	/	3 000 000	6 500 000	12 300 000	21 800 000	38 600 000
TOTAL ACTIF	/	/	/	6 030 000	8 944 000	14 158 000	23 072 000	39 286 000

FIGURE A.1 – Bilans de startup (Actif)

PASSIF										
En milliers DZD	RÉALISATION					PRÉVISIONS				
	N+1	N+2	N+3	N+4	N+5	N+1	N+2	N+3	N+4	N+5
CAPITAUX PROPRES										
Capital émis	/	/	/	/	/	2 000 000	2 000 000	2 000 000	2 000 000	2 000 000
Capital non appelé	/	/	/	/	/	/	/	/	/	/
Ecart de réévaluation	/	/	/	/	/	/	/	/	/	/
Primes et réserves- Réserves Consolidées	/	/	/	/	/	300 000	500 000	700 000	900 000	1 100 000
Résultat net- RN part du groupe	/	/	/	/	/	2 323 000	5 961 600	10 570 200	17 216 800	26 458 800
Autres capitaux propres- report à nouveau	/	/	/	/	/	/	/	/	/	/
Part de la société consolidante (1)	/	/	/	/	/	/	/	/	/	/
Capitaux propres	/	/	/	/	/	4 623 000	8 461 600	13 270 200	20 116 800	29 558 800
Emprunts et dettes financières	/	/	/	/	/	500 000	800 000	1 000 000	1 200 000	1 400 000
Impôt différé passif	/	/	/	/	/	/	/	/	/	/
Autres dettes non courantes	/	/	/	/	/	200 000	300 000	400 000	500 000	600 000
Provisions et produits constatés d'avance	/	/	/	/	/	/	/	/	/	/
Passifs Non-Courant	/	/	/	/	/	700 000	1 100 000	1 400 000	1 700 000	2 000 000
Fournisseurs et comptes rattachés	/	/	/	/	/	300 000	500 000	800 000	1 200 000	1 800 000
Impôts	/	/	/	/	/	120 000	250 000	400 000	600 000	800 000
Autres dettes	/	/	/	/	/	160 000	260 000	420 000	620 000	920 000
Trésorerie passif	/	/	/	/	/	130 000	372 400	1 868 800	3 635 200	4 207 200
Passifs Courants	/	/	/	/	/	710 000	1 382 400	3 488 800	6 055 200	7 727 200
Total Passif	/	/	/	/	/	6 030 000	8 944 000	14 158 000	23 072 000	39 286 000
Vérification de l'équilibre Actif/Passif	/	/	/	/	/	OK	OK	OK	OK	OK

FIGURE A.2 – Bilans de startup (PASSIF)

TABLEAU DE CALCUL DES RÉSULTATS ATTENDUS										
(En milliers DZD)										
Poste	RÉALISATION					PRÉVISION				
	N+1	N+2	N+3	N+4	N+5	N+1	N+2	N+3	N+4	N+5
Vente et produits annexes 70	/	/	/	/	/	8 640 000	17 100 000	28 960 000	52 120 000	93 880 000
Variation des stocks produits finis et en cours 72	/	/	/	/	/	/	/	/	/	/
Production immobilisée 73	/	/	/	/	/	/	/	/	/	/
Subvention d'exploitation 74	/	/	/	/	/	/	/	/	/	/
Production de l'exercice	/	/	/	/	/	8 640 000	17 100 000	28 960 000	52 120 000	93 880 000
Achats consommés 60	/	/	/	/	/	1 200 000	1 500 000	1 900 000	2 300 000	2 800 000
Services extérieurs et autres consommations 61/62	/	/	/	/	/	1 930 000	2 660 000	3 420 000	4 170 000	4 920 000
Consommation de l'exercice	/	/	/	/	/	3 130 000	4 160 000	5 320 000	6 470 000	7 720 000
Valeur ajoutée d'exploitation	/	/	/	/	/	5 510 000	12 940 000	23 640 000	45 650 000	86 160 000
Charges de personnel 63	/	/	/	/	/	340 000	1 040 000	1 240 000	1 460 000	1 890 000
Impôts et taxes et versement assimilés 64	/	/	/	/	/	120 000	180 000	260 000	350 000	500 000
Excédent Brut d'Exploitation	/	/	/	/	/	5 050 000	11 720 000	22 840 000	43 840 000	83 770 000
Autres produits opérationnels 75	/	/	/	/	/	/	/	/	/	/
Autres charges opérationnelles 65	/	/	/	/	/	/	/	/	/	/
Dotations aux amortissements, provisions 68	/	/	/	/	/	566 000	566 000	566 000	566 000	566 000
Reprise sur pertes de valeurs et provisions 78	/	/	/	/	/	/	/	/	/	/
Résultat opérationnel	/	/	/	/	/	4 484 000	11 154 000	21 574 000	43 274 000	83 204 000
Produits financiers 76	/	/	/	/	/	/	/	/	/	/
Charges financières 66	/	/	/	/	/	50 000	60 000	80 000	100 000	120 000
Résultat financier	/	/	/	/	/	-50 000	-60 000	-80 000	-100 000	-120 000
Résultat Ordinaire avant impôt	/	/	/	/	/	4 434 000	11 094 000	21 494 000	43 174 000	83 084 000
Impôt exigible sur résultat ordinaire	/	/	/	/	/	665 100	1 664 100	3 224 100	6 476 100	12 462 600
Impôt différé (variation) sur résultat ordinaire	/	/	/	/	/	/	/	/	/	/
TOTAL DES PRODUITS DES ACTIVITÉS ORDINAIRES	/	/	/	/	/	8 640 000	17 100 000	28 960 000	52 120 000	93 880 000
TOTAL DES CHARGES DES ACTIVITÉS ORDINAIRES	/	/	/	/	/	4 871 100	6 005 900	7 465 100	8 946 100	10 796 600
RÉSULTAT NET DES ACTIVITÉS ORDINAIRES	/	/	/	/	/	3 768 900	11 094 100	21 494 100	43 173 900	83 083 400
Éléments extraordinaires (produits)	/	/	/	/	/	/	/	/	/	/
Éléments extraordinaires (charges)	/	/	/	/	/	/	/	/	/	/
Résultat extraordinaire	/	/	/	/	/	/	/	/	/	/
RÉSULTAT NET DE L'EXERCICE	/	/	/	/	/	3 768 900	11 094 100	21 494 100	43 173 900	83 083 400

FIGURE A.3 – Comptes de résultat attendus.

Comptes du Trésor										
(En milliers DZD)										
Catégories	RÉALISATION					PRÉVISION				
	N+1	N+2	N+3	N+4	N+5	N+1	N+2	N+3	N+4	N+5
Flux net de trésorerie provenant des activités opérationnelles										
Résultat net de l'exercice	/	/	/	/	/	3 768 900	11 094 100	21 494 100	43 173 900	83 083 400
Ajustements pour :										
Amortissements et provisions	/	/	/	/	/	566 000	566 000	566 000	566 000	566 000
Variation des impôts différés	/	/	/	/	/	/	/	/	/	/
Variation des stocks	/	/	/	/	/	/	/	/	/	/
Variation des clients et autres créances	/	/	/	/	/	/	/	/	/	/
Variation des fournisseurs et autres dettes	/	/	/	/	/	/	/	/	/	/
Plus ou moins-values de cession, nettes d'impôts	/	/	/	/	/	/	/	/	/	/
Flux de trésorerie générés par l'activité (A)	/	/	/	/	/	4 334 900	11 660 100	22 060 100	43 739 900	83 649 400
Flux net de trésorerie provenant des activités d'investissement										
Décassements sur acquisition d'immobilisations	/	/	/	/	/	-2 830 000	-2 264 000	-1 698 000	-1 132 000	-566 000
Encaissements sur cession d'immobilisations	/	/	/	/	/	/	/	/	/	/
Incidence des variations de périmètre de consolidation (1)	/	/	/	/	/	/	/	/	/	/
Flux de trésorerie liés aux opérations d'investissement (B)	/	/	/	/	/	-2 830 000	-2 264 000	-1 698 000	-1 132 000	-566 000
Flux net de trésorerie provenant des opérations de financement										
Dividendes versés aux actionnaires	/	/	/	/	/	/	/	/	/	/
Augmentation de capital	/	/	/	/	/	2 000 000	0	0	0	0
Emprunts	/	/	/	/	/	300 000	200 000	200 000	150 000	100 000
Remboursements d'emprunts	/	/	/	/	/	-50 000	-80 000	-100 000	-120 000	-150 000
Flux de trésorerie liés aux opérations de financement (C)	/	/	/	/	/	2 250 000	120 000	100 000	30 000	-50 000
Variation de trésorerie et équivalents de trésorerie de la période (A+B+C)	/	/	/	/	/	3 754 900	9 516 100	20 462 100	42 637 900	83 033 400
Solde de trésorerie d'ouverture (Début de la période)	/	/	/	/	/	500 000	4 254 900	13 771 000	34 233 100	76 871 000
Trésorerie de clôture (Fin de période)	/	/	/	/	/	4 254 900	13 771 000	34 233 100	76 871 000	159 904 400
Variation de trésorerie	/	/	/	/	/	3 754 900	9 516 100	20 462 100	42 637 900	83 033 400

(1) Incidence des variations de périmètre de consolidation : Non applicable dans le cadre de ce projet.

FIGURE A.4 – Flux de trésorerie consolidés

Annexe B

B.1 Modèle d'affaires :

B.1.1 Business Model Canvas :

C'est un outil stratégique qui permet de représenter de manière simple et visuelle le modèle économique d'un projet à travers 9 blocs interdépendants qui décrivent la manière dont l'entreprise crée, délivre et capte de la valeur. Présenté sous la forme d'une matrice sur une seule page pour faciliter l'analyse et la prise de décision. **Les 9 blocs** : Partenariats clés, Activités clés, Proposition de valeur, Relation client, Segments de clientèle, Ressources clés, Canaux de distribution, Structure de coûts, Sources de revenus.

B.1.2 BMC permet :

- D'avoir une vision globale du projet et de son modèle économique.
- D'identifier les éléments clés nécessaires au succès du projet.
- De faciliter la prise de décision et la planification stratégique.
- D'améliorer la communication et la coordination au sein de l'équipe.
- De soutenir le lancement et le développement d'un nouveau produit ou service.

B.1.3 Le BMC de notre projet :



FIGURE B.1 – Le Business Model Canvas