الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université de 8 Mai 1945 – Guelma -

Faculté de Mathématiques, d'Informatique et de Sciences de la Matière

Département : d'Informatique

Mémoire de Fin d'études Master

Filière : Informatique

Option : Systèmes Informatiques

Thème :

Un Système de Détection D'Intrusion pour les Smart Grids

Encadré Par :

Mme Baalia Saida

Présenté par :

Zitouni Nada

Membres du Jury :

Dr. Ouarda ZEDADRA

Dr. Hiba Abdelmoumen

Septembre 2024

REMERCIEMENTS

Je veux exprimer par ces quelques lignes de remerciement notre gratitude envers tous ceux en qui par leur présence, leur soutien, leur disponibilité et leurs conseils, nous avons eu courage d'accomplir ce travail.

Avant tout ; je remercie Dieu de j'avoir Aidé à faire ce mémoire.

Je tiens à adresser mes chaleureux remerciements à ma encadreur Madame Baalia Saida qui m'a aidé à élaborer ce travail par ses conseils et soutien durant toute la période de l'encadrement. Je remerciements à tous les membres de jury pour l'honneur qu'ils j'ai fait en acceptant d'examiner ce mémoire. Je remerciements à mes enseignants qui ont contribué à notre formation.

Je remerciements à tous ceux qui m'ont aidé de près ou de loin à réaliser ce mémoire et à élaborer ce travail.

Merci

Résumé :

Les réseaux électriques traditionnels, avec une communication unidirectionnelle, manquent de flexibilité et de gestion efficace des pannes. En revanche, les Smart Grids intègrent des technologies avancées, permettant une gestion bidirectionnelle de l'énergie et une meilleure adaptation aux besoins, tout en optimisant l'intégration des énergies renouvelables. Cependant, leur interconnexion les rend vulnérables aux cyberattaques, ce qui peut entraîner des pannes et des risques pour les infrastructures critiques. Sécuriser ces réseaux est donc essentiel. Ce mémoire propose un système de détection d'intrusion basé sur l'apprentissage automatique, combinant CNN et LSTM, pour améliorer la sécurité des Smart Grids. Testé sur le dataset KDD99, le modèle a montré de bonnes performances en termes de précision, dépassant les méthodes existantes.

Mots-clés : Smart Grid, un système de détection d'intrusion, le Deep Learning, cyberattaques.

Abstract:

Traditional power grids, with one-way communication, lack flexibility and efficient fault management. On the other hand, Smart Grids integrate advanced technologies, allowing bidirectional energy management and better adaptation to needs, while optimizing the integration of renewable energies. However, their interconnection makes them vulnerable to cyberattacks, which can lead to outages and risks for critical infrastructures. Securing these networks is therefore essential. This thesis proposes an intrusion detection system based on machine learning, combining CNN and LSTM, to improve the security of Smart Grids. Tested on the KDD99 dataset, the model showed good performance in terms of accuracy, outperforming existing methods.

Keywords: Smart Grid, an intrusion detection system, Deep Learning, cyberattacks.

ملخص

تفتقر شبكات الطاقة التقليدية، ذات الاتصال أحادي الاتجاه، إلى المرونة والإدارة الفعالة للانقطاع. ومن ناحية أخرى، تعمل الشبكات الذكية على دمج التقنيات المتقدمة، مما يسمح بإدارة الطاقة ثنائية الاتجاه والتكيف بشكل أفضل مع الاحتياجات، مع تحسين تكامل الطاقات المتجددة. ومع ذلك، فإن ترابطها يجعلها عرضة للهجمات الإلكترونية، مما قد يؤدي إلى انقطاع الخدمة ومخاطر البنية التحتية الحيوية. ولذلك فإن تأمين هذه الشبكات أمر ضروري. تقترح هذه الأطروحة نظام كشف التسلل القائم على التعلم الآلي، والجمع بين CNN وLSTM، لتحسين أمن الشبكات الذكية. تم اختبار النموذج على مجموعة بيانات KDD99، وأظهر أداءً جيدًا من حيث الدقة، متفوقًا على الأساليب الحالية.

الكلمات المفتاحية: الشبكة الذكية، نظام كشف التسلل، التعلم العميق، الهجمات الإلكترونية.

Table des matières :

Liste de figures

Chapitre I :

Chapitre III :

Liste de tableaux

Chapitre III

Chapitre IV

Liste des Abréviations

- IA : Intelligence artificielle
- CNN : Réseau neuronal convolutif
- DL : Deep Learning
- IDS : Système de détection d'intrusion
- LSTM : Mémoire à long terme
- ML : Machine Learning
- SG : Smart Grid
- TPR : Taux de vrais positifs
- FPR : Taux de faux positifs
- ROC : Caractéristique de fonctionnement du récepteur
- AUC : Aire sous la courbe
- API : Interface de programmation d'applications
- CSV : Valeurs séparées par des virgules
- SVM : Machine à vecteurs de support
- ReLU : Unité linéaire rectifiée
- F1-Score : Score F1
- ROC-AUC : Caractéristique de fonctionnement du récepteur - Aire sous la courbe
- TP : True Positives
- TN : True Negatives
- FP : False Positives
- FN : False Negatives
- RMSE : Root Mean Square Error
- EH_WSN : Energy Harvesting Wireless Sensor Network
- 6LoWPAN : IPv6 over Low-Power Wireless Personal Area Networks
- GA : algorithme génétique

Introduction Générale

Au cours des dernières décennies, les avancées des technologies de l'information et de la communication (TIC) ont révolutionné divers secteurs, dont celui de l'énergie. L'émergence des Smart Grids représente une évolution significative par rapport aux réseaux électriques traditionnels. Ces nouveaux réseaux permettent une gestion plus dynamique et plus efficace de la distribution d'électricité grâce à l'intégration des TIC [1]. Les Smart Grids facilitent l'intégration des sources d'énergie renouvelables, améliorent la gestion de la demande et réduisent les pertes d'énergie, contribuant ainsi à un avenir énergétique plus durable et résilient. Cette avancée technologique s'accompagne de nouveaux défis, notamment en termes de sécurité. L'interconnexion et la complexité accrues des Smart Grids les exposent à des risques importants de cyberattaques, mettant en péril la fiabilité et la sécurité de l'approvisionnement en électricité. La sécurité des systèmes informatiques au sein des Smart Grids est donc devenue une préoccupation majeure. Les attaques potentielles peuvent aller d'intrusions basiques à des cyberattaques sophistiquées, capables de perturber le fonctionnement global du réseau.

L'objectif principal de cette mémoire est de concevoir et implémenter un système de détection d'intrusion (IDS) efficace pour les Smart Grids. Ce système identifier et neutraliser les attaques avant qu'elles n'affectent sérieusement le réseau. Plus précisément, nos recherches portent sur le développement d'un modèle de détection basé sur une combinaison de réseaux de neurones convolutifs (CNN) et de réseaux de neurones récurrents (LSTM). Cette approche hybride est choisie pour tirer parti des capacités des CNN à détecter des motifs locaux dans les données et des LSTM à modéliser les dépendances temporelles, offrant ainsi une solution robuste contre les différentes attaques auxquelles les Smart Grids peuvent être exposés.

La mémoire est structurée autour de quatre chapitres, chacun fournir une compréhension approfondie des aspects théoriques et pratiques de la sécurité des SG :

Chapitre I : Smart Grid

Ce chapitre présente les bases des SG, en expliquant leur fonctionnement, leur architecture et leur importance dans le contexte énergétique actuel. Il met les composants technologiques qui les rendent plus efficaces et plus fiables.

Chapitre II : Sécurité des réseaux dans les Smart Grids

Nous abordons ici les concepts fondamentaux de la sécurité informatique appliqués aux SG, en présentant les types d'attaques possibles, les outils de sécurité existants et les bases nécessaires à la compréhension des menaces qui pèsent sur les SG.

Chapitre III : Systèmes de détection d'intrusions

Ce chapitre se concentre sur le concept de systèmes de détection d'intrusions (IDS) et leur rôle de défense contre les cyberattaques. Nous discutons des défis spécifiques de la sécurité dans les SG et des approches existantes pour classer les attaques.

Chapitre IV : Conception et implémentation

Ce chapitre décrit en détail la conception et l'implémentation du modèle de détection d'intrusions proposé. Nous explorons l'architecture du modèle CNN-LSTM, les étapes d'apprentissage, les environnements de développement utilisés, ainsi que les résultats obtenus à travers différents tests. Les performances du modèle sont comparées à celles des approches existantes pour évaluer son efficacité.

Notre mémoire se termine par une conclusion générale qui résume les principales contributions de notre recherche. Nous discutons également des perspectives d'avenir, notamment les possibilités d'amélioration du modèle de détection d'intrusion, d'intégration de nouvelles techniques d'apprentissage automatique et d'élargissement de l'application de ce modèle à d'autres domaines de la sécurité informatique.

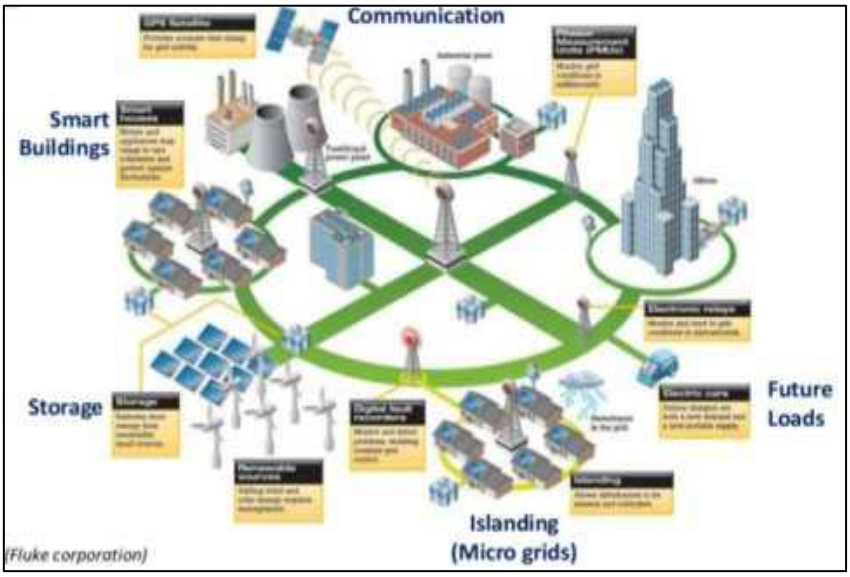
Chapitre I : Smart Grid

I.1 Introduction

On va présenter dans ce chapitre les bases de la compréhension des technologies et des structures qui composent les Smart Grids, en soulignant les avantages qu'ils offrent en termes d'efficacité énergétique et de gestion de la demande.

I.2 Définition :

Les Smart Grids, ou réseaux électriques intelligents, sont des systèmes de distribution d'électricité qui utilisent des technologies de l'information et de la communication pour optimiser la production, la distribution et la consommation d'énergie. Contrairement aux réseaux électriques traditionnels, les Smart Grids permettent une interaction bidirectionnelle entre les fournisseurs d'énergie et les consommateurs, facilitant ainsi une gestion plus efficace et adaptative de l'énergie. En intégrant des capteurs avancés, des dispositifs de contrôle et des technologies de communication, les Smart Grids sont capables de surveiller et de répondre en temps réel aux fluctuations de la demande et de l'offre d'électricité. Cette capacité de réponse dynamique aide à améliorer la fiabilité du réseau, à réduire les pertes d'énergie et à intégrer de manière plus efficace les sources d'énergie renouvelable [2].



FigureI.1 : Smart Grid [3]

I.3 Architecture des Smart Grids

Dans [3] les auteurs ont proposé une architecture composée principalement de trois niveaux : l'infrastructure du réseau électrique, les structures de données de communication et de détection, et les systèmes de gestion.

a) Niveau 1 : Infrastructure du réseau électrique

À la base de l'architecture des Smart Grids se trouve l'infrastructure du réseau électrique traditionnel, qui comprend les générateurs d'électricité, les lignes de transmission et les réseaux de distribution. Dans le cadre des Smart Grids [4], cette infrastructure est enrichie par des technologies avancées telles que les capteurs intelligents, les compteurs intelligents et les dispositifs de contrôle automatisés. Ces technologies permettent une surveillance et un contrôle en temps réel de l'état du réseau, facilitant une gestion plus efficace de l'énergie et une détection rapide des problèmes.

b) Niveau 2 : Structures de données de communication et de détection

D'après [5] Le deuxième niveau de l'architecture des Smart Grids est constitué des structures de données de communication et de détection. Ce niveau intègre des technologies de l'information et de la communication (TIC) pour assurer la collecte, la transmission et le traitement des données en temps réel. Les réseaux de communication bidirectionnels permettent aux opérateurs de surveiller les performances du réseau et aux consommateurs de participer activement à la gestion de leur

consommation d'énergie. Les systèmes de détection jouent un rôle crucial dans l'identification des anomalies et des cybermenaces, garantissant ainsi la sécurité et la résilience du réseau.

c) Niveau 3 : Systèmes de gestion

Le troisième niveau de l'architecture des Smart Grids [6], comprend les systèmes de gestion, qui orchestrent l'ensemble du réseau électrique intelligent. Ces systèmes utilisent des algorithmes avancés de gestion de l'énergie et de l'apprentissage automatique pour optimiser la production, la distribution et la consommation d'électricité. Ils permettent une prise de décision rapide et efficace, améliorant la stabilité et la fiabilité du réseau. Les systèmes de gestion des données énergétiques (EMS) et les systèmes de gestion de la distribution (DMS) sont des exemples de technologies utilisées à ce niveau pour superviser et contrôler les opérations du réseau.

Selon [7] L'architecture des Smart Grids repose sur une infrastructure robuste enrichie par des technologies de communication avancées et des systèmes de gestion intelligents. Cette structure intégrée permet une gestion plus dynamique et efficace de l'énergie, tout en renforçant la résilience et la sécurité du réseau électrique.

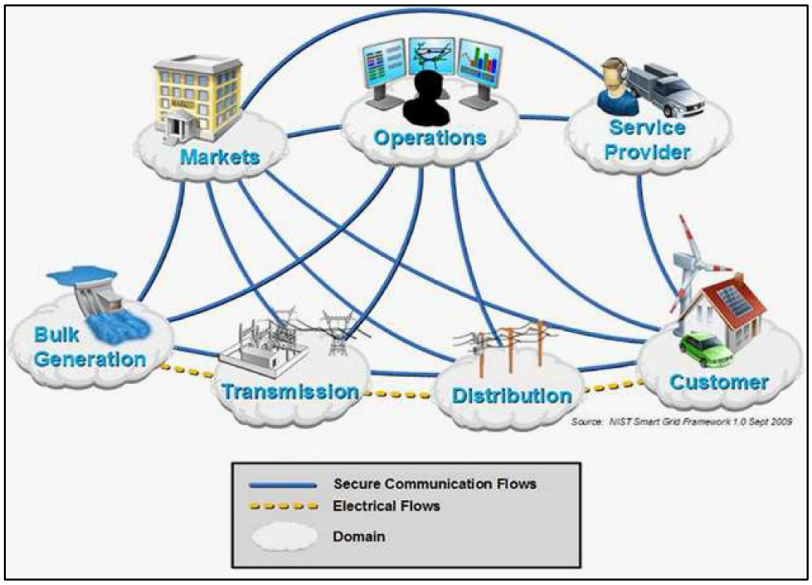


Figure I.2 : Modèle conceptuel du réseau intelligent [8]

I.4 Les composants des Smart Grids

Les SG intègrent des composants essentiels qui travaillent de concert pour créer un réseau électrique intelligent et adaptatif ; pour surveiller, contrôler et optimiser la production, la distribution et la consommation d'électricité. Les principaux composants [9]des Smart Grids sont :

a. Compteurs Intelligents :

Les compteurs smart, connus sous le nom avancés ou communicants, sont des dispositifs électroniques installés chez les consommateurs pour mesurer et transmettre les données de consommation d'énergie en temps réel. Ils permettent une gestion plus précise de la demande d'électricité et facilitent la tarification dynamique en fonction des fluctuations d'offre et demande.

b. Capteurs Intelligents :

Les smart capteurs sont des dispositifs de surveillance distribués à travers le réseau électrique pour collecter des données sur les conditions opérationnelles et environnementales. Ils mesurent les paramètres « la tension, le courant, la température » et les conditions météorologiques, permettant une surveillance en temps réel de l'état du réseau et une détection précoce des anomalies.

c. Dispositifs de Contrôle Automatisé :

Les dispositifs de contrôle automatisé, les interrupteurs, les disjoncteurs et les régulateurs de tension, sont utilisés pour contrôler la distribution d'électricité et optimiser la gestion des flux d'énergie. Ils permettent une intervention rapide en cas de perturbations du réseau, minimisant ainsi les temps d'arrêt et améliorant la fiabilité du système [10].

d. Réseaux de Communication Bidirectionnelle :

Ils permettent l'échange d'informations entre les différents composants des SG, y compris les compteurs smart, les capteurs et les dispositifs de contrôle. Ils facilitent la collecte et la transmission des données en temps réel, ainsi que la coordination des opérations sur l'ensemble du réseau [11].

e. Systèmes de Gestion de l'Énergie :

Les systèmes de gestion d'énergie des données énergétiques (EMS) et les systèmes de gestion du distribution (DMS), sont utilisés pour superviser et contrôler les opérations du réseau électrique. Ils utilisent des algorithmes avancés pour optimiser la production, la distribution et la consommation d'électricité, en fonction des conditions du marché et des contraintes opérationnelles [12].

I.5 Organisation d'un Smart Grid

Selon [13] Dans un Smart Grid, l'organisation des différents réseaux joue un rôle crucial dans la fourniture efficace et fiable de l'électricité. Cette organisation repose sur une architecture hiérarchique qui intègre plusieurs niveaux de réseaux pour répondre aux besoins diversifiés de distribution d'énergie.

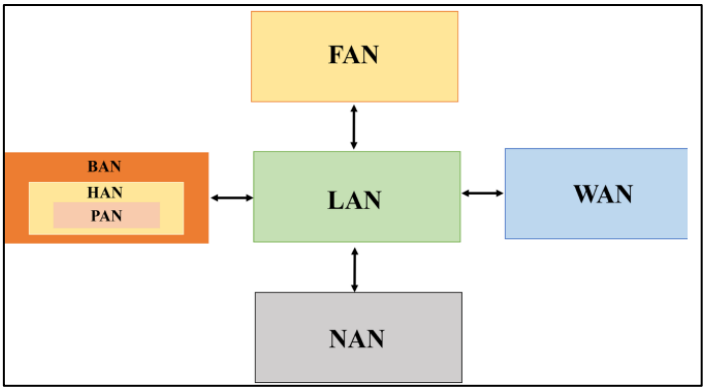


Figure I.3 : Différents réseaux de communication dans les réseaux intelligents [13].

- **Réseau Domestique (HAN - Home Area Network) :**

Le réseau domestique, ou HAN, constitue le premier niveau de l'organisation des Smart Grids. Il englobe les équipements et les appareils électriques installés dans les foyers et les bâtiments, tels que les compteurs intelligents, les thermostats intelligents, les appareils électroménagers connectés, etc... Ce réseau permet une communication bidirectionnelle entre les équipements et les fournisseurs de services énergétiques, facilitant ainsi la surveillance et le contrôle de la consommation d'énergie au niveau résidentiel [14].

- **Réseau de Jonction Extérieure (FAN - Field Area Network) :**

Le réseau de jonction extérieure, ou FAN, constitue le deuxième niveau de l'organisation des Smart Grids. Il relie les équipements de terrain, tels que les transformateurs, les postes de distribution et les dispositifs de contrôle automatisé, aux systèmes de contrôle et de gestion centralisés [13]. Ce réseau assure la transmission sécurisée des données entre les équipements de terrain et les centres de contrôle, permettant ainsi une surveillance en temps réel de l'état du réseau et une coordination efficace des opérations.

- **Réseau de Proximité (NAN - Neighborhood Area Network) :**

Le réseau de proximité, ou NAN, constitue le troisième niveau de l'organisation des Smart Grids. Il agit comme une interface entre les réseaux de distribution de basse tension et les réseaux de transmission à haute tension. Ce réseau facilite la gestion des flux d'énergie au niveau local, en optimisant la distribution de l'électricité et en minimisant les pertes d'énergie sur de courtes distances. Ces différents réseaux forment une architecture robuste et évolutive qui permet une gestion efficace et intelligente de l'électricité. L'organisation stratégique des Smart Grids garantit une fourniture d'énergie fiable, résiliente et adaptative, tout en répondant aux besoins changeants des consommateurs et en favorisant l'intégration des énergies renouvelables [15].

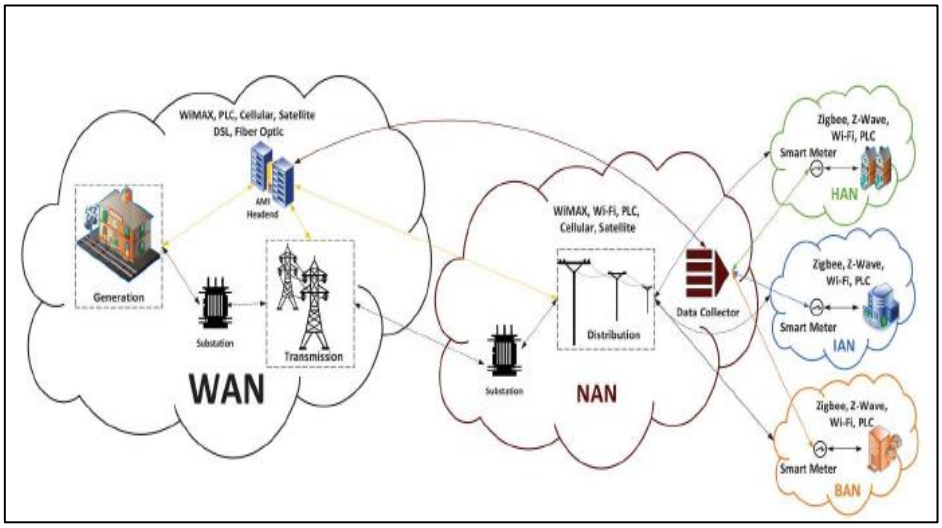


Figure I.4 : L'architecture de communication du système SG [15].

I.6 Les Facteurs Majeurs dans les Smart Grids

Les Smart Grids sont soumis à divers facteurs qui influent sur leur conception, leur déploiement et leur efficacité opérationnelle sont :

- L'évolution rapide des technologies de l'information et de la communication (TIC) joue un rôle majeur dans le développement des Smart Grids. Les avancées telles que l'Internet des objets (IoT) [16], les capteurs intelligents, et les systèmes de gestion de l'énergie permettent une surveillance et un contrôle avancés du réseau électrique. Cette évolution technologique ouvre la voie à de nouvelles fonctionnalités, telles que la détection d'anomalies en temps réel, la gestion dynamique de la charge, et l'intégration transparente des énergies renouvelables.

- Durabilité Environnementale, La transition vers des Smart Grids est également motivée par des préoccupations croissantes en matière de durabilité environnementale. En intégrant des sources d'énergie renouvelable et en optimisant l'utilisation des ressources énergétiques, les Smart Grids réduire leur empreinte carbone et à promouvoir une production d'énergie plus propre et plus respectueuse de l'environnement [17]. Cette orientation vers la durabilité contribue à atténuer les effets du changement climatique tout en assurant la disponibilité continue de l'énergie pour les générations futures.

- La Fiabilité du Réseau électrique est un facteur essentiel dans la conception des Smart Grids. En améliorant la surveillance et la gestion des actifs, ainsi que la détection et la réponse aux pannes, les Smart Grids visent à accroître la fiabilité et la résilience du réseau électrique. Cela implique la mise en place de mécanismes avancés de détection d'anomalies, de restauration automatique, et de planification de la capacité pour garantir une alimentation électrique continue et stable [18].

I.7 Les avantages des Smart Grids

Les Smart Grids offrent d'avantages qui transcendent les systèmes électriques traditionnels.

- Efficacité Énergétique des Smart Grids permettent une utilisation plus efficace de l'énergie en intégrant des technologies avancées de gestion de la demande et de distribution. Grâce à la collecte de données en temps réel et à l'optimisation de la charge, les Smart Grids réduisent les pertes d'énergie et améliorent l'efficacité globale du système électrique [19].

- Selon [20] Les Smart Grids facilitent l'intégration harmonieuse des sources d'énergie renouvelable, telles que l'énergie solaire et éolienne, dans le réseau électrique. En permettant une gestion dynamique de la production et de la consommation, ils favorisent l'utilisation accrue des énergies propres et renouvelables, réduisant ainsi la dépendance aux combustibles fossiles.

- Les Smart Grids permettent une gestion proactive de la demande d'électricité en incitant les consommateurs à ajuster leur consommation en fonction des fluctuations de l'offre et de la demande. Grâce à des tarifs différenciés et à des incitations à l'efficacité énergétique, ils encouragent une utilisation plus rationnelle de l'énergie et réduisent les pics de demande [21].

- En intégrant des technologies avancées de surveillance et de contrôle, les Smart Grids améliorent la fiabilité et la résilience du réseau électrique. Ils permettent une détection précoce des pannes, une restauration rapide du service, et une meilleure gestion des situations d'urgence, garantissant ainsi une alimentation électrique plus fiable pour les consommateurs [22].

- Les Smart Grids facilitent une interaction bidirectionnelle entre les fournisseurs d'énergie et les consommateurs. En permettant aux utilisateurs de devenir des producteurs d'énergie grâce à des installations solaires ou éoliennes domestiques, ils favorisent une participation active des consommateurs à la production et à la gestion de l'électricité [23].

1.8 Conclusion

Dans ce chapitre nous a permis de mieux comprendre les fondements des Smart Grids et les raisons pour lesquelles ils représentent une avancée significative dans la gestion de l'énergie.

Les Smart Grids offrent une gamme étendue d'avantages, allant de l'efficacité énergétique à la résilience du réseau, en passant par l'intégration des énergies renouvelables et la gestion de la demande. Leur adoption et leur déploiement contribuent à transformer les systèmes électriques traditionnels en des infrastructures plus intelligentes, durables et adaptatives.

Dans les chapitres suivants, nous explorerons en détail les aspects liés à la sécurité des Smart Grids et proposerons des solutions pour renforcer leur protection contre les attaques

Chapitre II La Sécurité dans les Smart Grid

II.1 Introduction

Dans ce chapitre deux, nous présenterons les différents types d'attaques et les concepts fondamentaux de la sécurité informatique, et les différents outils de sécurité dans les SG. Par la suite, dans le troisième chapitre, nous traiterons ces intrusions en utilisant des systèmes de détection d'intrusion

II.2.1 Définition Une attaque informatique :

Dans [24], Une attaque informatique est une tentative délibérée et malveillante de compromettre un système informatique, ses données ou ses utilisateurs. Ces attaques peuvent prendre diverses formes, telles qu'un accès non autorisé, la destruction de données critiques ou la manipulation des opérations normales d'un système. Ils exploitent les vulnérabilités des logiciels, des réseaux ou des pratiques de sécurité pour causer des dommages financiers, perturber les opérations, voler des informations sensibles ou nuire à la réputation d'une organisation.

II.2.2 Type d'Attaques Informatiques :

Les SG, en raison de leur complexité et de leur interconnexion étendue, sont vulnérables à divers types d'attaques que ces systèmes peuvent être susceptibles d'inclure [25] :

a) Attaques par déni de service (DoS) :

Une attaque visant à rendre un ordinateur inopérant en l'inondant de trafic superflu. Par exemple, un serveur qui se trouve entièrement occupé à traiter de fausses demandes de connexion. Des machines peuvent être responsables de cette attaque, souvent sans que leurs propriétaires en aient connaissance.

b) Attaque de l'homme du milieu :

Le pirate s'installe entre deux ordinateurs et feint d'être l'un d'eux pour obtenir le mot de passe de l'autre. Il peut ensuite se retourner contre le premier en utilisant un mot de passe valide pour l'attaquer.

c) Sniffing :

Il s'agit d'écouter une ligne de transmission par laquelle circulent des données afin de les capturer en temps réel. Cette méthode peut être employée en interne pour le débogage ou de manière malveillante par un individu malintentionné cherchant, par exemple, à obtenir un mot de passe. Elle vise principalement à intercepter des données non chiffrées. Dans certains réseaux (non commutés, connectés via un concentrateur ou des câbles coaxiaux), tous les messages sont envoyés à l'ensemble des utilisateurs. En modifiant l'état de l'interface réseau (c'est-à-dire en activant le mode espion), l'attaquant peut capter toutes les communications pour les examiner.

d) Spoofing :

La technique de « spoofing » désigne une méthode d'intrusion qui consiste à transmettre à un serveur des paquets semblant émaner d'une adresse IP reconnue par le pare-feu. Le pirate rend la machine inaccessible afin d'intercepter les codes de communication et d'établir une connexion non autorisée.

II.2.3 Classification des attaques

Les attaques informatiques sur les Smart Grids peuvent être classées en deux types principaux en fonction de leur impact : les attaques passives et les attaques actives.

a) Attaques passives :

Les attaques passives consistent à intercepter et à écouter les communications sans altérer les données ou les opérations du réseau. L'objectif principal de l'attaquant est d'obtenir des informations sensibles transitant par le réseau [26]. Ces attaques sont généralement indétectables car elles n'entraînent aucune modification visible des actifs.

Des exemples d'attaques passives incluent l'interception de données et l'espionnage des communications :

- Interception de données : capture des données transmises sur le réseau pour recueillir des informations telles que la consommation d'énergie, les informations sur les utilisateurs ou les configurations du réseau.
- Espionnage des communications : Écoute des communications entre les différents composants du Smart Grid, comme les échanges entre capteurs et systèmes de contrôle, pour collecter des informations stratégiques.

b) Attaques actives :

Les attaques actives provoquer un changement significatif dans le fonctionnement du système, comme la modification des données, l'interférence avec les communications ou l'interruption du service.

Des exemples d'attaques actives incluent l'injection de faux messages, le déni de service (DoS) et la modification des configurations [27] :

- Injection de faux messages : envoi de messages falsifiés dans le réseau pour perturber les opérations du Smart Grid, comme l'envoi de fausses commandes aux appareils de terrain.
- Déni de service (DoS) : Saturation des ressources du réseau ou des systèmes de contrôle pour empêcher les services de fonctionner correctement, provoquant des pannes ou des ralentissements.
- Modification des configurations : Modification des configurations des équipements ou des paramètres de contrôle pour déstabiliser le fonctionnement du réseau et provoquer des dysfonctionnements.

II.2.4 Les Motivations d'une Attaque

Comprendre les motivations des cyberattaques est obligatoire pour que les organisations puissent anticiper les types de menaces auxquelles elles peuvent être confrontées et mettre en œuvre des mesures de sécurité appropriées. Quelques motivations clés pour les attaques [28] :

- **Gain financier :**

- Vol de données, les attaquants peuvent voler des informations sensibles, telles que des numéros de carte de crédit, des coordonnées bancaires ou des données personnelles, pour les revendre sur le marché noir ou les utiliser à des fins de fraude financière.

- Ransomware, Les logiciels malveillants peuvent être utilisés pour chiffrer les données de la victime, les attaquants exigeant une rançon pour le décryptage.

- Fraude, Les cybercriminels peuvent manipuler les systèmes pour détourner des fonds ou effectuer des transactions frauduleuses.

- **Espionnage :**

- Espionnage industriel, les entreprises peuvent être ciblées pour voler des secrets commerciaux, des recherches en cours, des brevets ou des plans stratégiques.

- Espionnage politique ou militaire, les gouvernements peuvent mener des cyberattaques pour obtenir des informations sensibles sur les capacités militaires, les stratégies politiques ou les négociations diplomatiques d'autres pays.

- **Motifs politiques ou idéologiques :**

- Piratage, des groupes ou des individus peuvent lancer des cyberattaques pour protester contre des politiques, des pratiques ou des organisations qu'ils jugent inacceptables. Cela peut inclure la dégradation de sites Web ou la publication de données sensibles.

- Terrorisme, Les cyberattaques peuvent être utilisées pour provoquer des perturbations majeures ou intimider les populations dans le cadre d'une campagne terroriste.

- **Vengeance personnelle ou ressentiment :**

- Employés mécontents, un employé actuel ou ancien peut exercer des représailles pour un traitement injuste en lançant une attaque visant à nuire à l'entreprise.

- Rivalités personnelles, les individus peuvent attaquer les systèmes pour régler des conflits personnels.

- **Désir de reconnaissance ou de défi artistique :**

- Concurrence, Certains hackers sont motivés par un défi technique ou cherchent à se faire reconnaître au sein de la communauté des hackers.

- Démonstration de compétences, les individus peuvent mener des attaques pour mettre en valeur leurs capacités techniques et acquérir une réputation.

- **Accès non autorisé aux ressources ou services :**

- Utilisation illégale, les attaquants peuvent chercher à utiliser les ressources de l'organisation, telles que la puissance de calcul ou la bande passante, à leurs propres fins, par exemple pour extraire des cryptomonnaies ou héberger du contenu illicite.

- Sabotage, les cyberattaques peuvent perturber ou à détruire des services ou des infrastructures critiques, comme des réseaux électriques ou des systèmes de contrôle industriel, afin de provoquer des dommages ou des perturbations.

II.3 La Sécurité Informatique

II.3.1 Définition :

La cybersécurité comprend toutes les mesures prises pour réduire la vulnérabilité d'un système aux menaces accidentelles ou intentionnelles. Il est essentiel d'identifier les exigences de base en matière de cybersécurité. Ils définissent les attentes des utilisateurs de systèmes informatiques en matière de sécurité [29].

II.3.2 Les Services, Les attaques et les mécanismes du Sécurité Informatique :

Une politique de sécurité informatique assurer la protection des données et des réseaux d'une entreprise contre diverses menaces. Pour atteindre cet objectif, plusieurs services de sécurité sont mis en place, tels que la confidentialité, l'intégrité, la disponibilité, l'authentification et le contrôle d'accès. Ces services visent à sauvegarder les informations sensibles, à assurer leur exactitude, à les rendre accessibles aux utilisateurs autorisés et à vérifier l'identité des utilisateurs. Cependant, ces systèmes sont soumis à des menaces constantes provenant d'attaques informatiques telles que le phishing, les intrusions, les attaques par déni de service (DoS) et les logiciels malveillants. Afin de contrer ces menaces, des mécanismes de sécurité sont mis en place, notamment la cryptographie, le pare-feu, les systèmes de détection d'intrusion (IDS) et l'authentification multifacteur (MFA). Ces mesures contribuent à renforcer la sécurité des systèmes d'information et à réduire les risques liés aux cyberattaques [30].

II.3.2.1 La Disponibilité :

La disponibilité des données est primordiale pour garantir le bon fonctionnement du système d'information. L'objectif est de s'assurer que les services et les ressources sont accessibles en tout temps, permettant ainsi aux utilisateurs d'accéder aux informations au moment souhaité. Cela contribue à maintenir l'efficacité et la productivité de l'organisation en garantissant que les données sont disponibles lorsqu'elles sont nécessaires [31].

a) Les Attaques contre la Disponibilité

D'après [32] Les attaques contre la disponibilité rendre les services ou les ressources indisponibles pour les utilisateurs légitimes. Dans le contexte des Smart Grids, l'attaques peuvent gravement perturber la distribution et la gestion de l'énergie, entraînant des pannes de courant et des dysfonctionnements du réseau. Les attaques contre la disponibilité sont parmi les plus mauvais pour

les infrastructures des Smart Grids. Ces attaques peuvent prendre de nombreuses formes, incluant les attaques par déni de service distribué (DDoS), les attaques par déni de service (DoS), et les attaques physiques contre les équipements réseau.

b) **Types d'attaques contre la disponibilité** [33]:

- Attaques par déni de service distribué (DDoS) sur les Smart Grids inonder les serveurs ou les équipements réseau avec un volume massif de trafic, rendant les services indisponibles pour les utilisateurs légitimes.

- Attaques par déni de service (DoS), bien que similaires aux DDoS, sont souvent menées par un seul attaquant ou une seule machine, mais elles peuvent néanmoins causer des interruptions significatives des services.

- Les Attaques physiques impliquent la destruction ou la manipulation d'équipements réseau cruciaux, comme les transformateurs, les sous-stations, ou les câbles de communication.

c) Les mécanismes [33]:

- La Redondance implique la duplication des ressources critiques (serveurs, disques durs, etc.) pour éviter les points de défaillance uniques.

- La Sauvegardes régulières garantissent la récupération des données en cas de perte ou de corruption.

- Le Plan de reprise après sinistre (PRA) procédures et ressources pré-planifiées pour restaurer les services en cas d'incidents majeurs.

II.3.2.2 L'Intégrité :

L'intégrité des données est essentielle pour s'assurer qu'elles n'ont pas été altérées pendant leur transmission. Il est crucial de garantir que les informations reçues sont bien celles qui ont été envoyées, sans aucune altération. Cela permet de maintenir la confiance dans les données échangées et d'éviter toute manipulation indésirable [31].

a) Les Attaques contre L'Intégrité

Les attaques contre l'intégrité altérer les données ou les opérations des systèmes pour provoquer des comportements anormaux ou des prises de décision erronées. Ces attaques peuvent avoir des conséquences graves sur le fonctionnement et la fiabilité du réseau électrique. L'intégrité des données est cruciale pour les opérations des Smart Grids, car elle garantit que les informations utilisées pour le contrôle et la gestion du réseau sont exactes et fiables. Les attaques contre l'intégrité peuvent entraîner des dysfonctionnements du réseau, des pannes d'électricité et des pertes économiques importantes [32].

b) **Types d'attaques contre L'Intégrité** [33]:

- Injection de fausses données (False Data Injection Attacks, FDIA), Les attaques par injection de fausses données consistent à insérer des informations incorrectes dans le système pour fausser les mesures et provoquer des actions incorrectes de la part des systèmes de contrôle.

- Attaques par modification de configuration, ces attaques modifier les configurations des dispositifs et systèmes de contrôle pour altérer leur fonctionnement normal.

- Attaques sur les protocoles de communication, Ces attaques exploitent les vulnérabilités des protocoles de communication pour altérer les messages échangés entre les dispositifs du Smart Grid.

c) Les mécanismes [33]:

- La Sommes de contrôle vérifiez l'intégrité des données en comparant les sommes de contrôle calculées avant et après la transmission ou le stockage.

- La Fonctions de hachage générez des valeurs uniques pour chaque ensemble de données, facilitant ainsi la détection des modifications non autorisées.

- La Signatures numériques utilisez des algorithmes de hachage et des clés cryptographiques pour garantir que les données n'ont pas été modifiées et authentifiez l'origine des données.

II.3.2.3 La Confidentialité

La confidentialité est un autre aspect fondamental de la sécurité des données. Elle vise à restreindre l'accès aux ressources échangées uniquement aux personnes autorisées. En assurant que seules les personnes légitimes peuvent accéder aux informations sensibles, on protège la vie privée et on évite les fuites d'informations confidentielles [31].

a) Les Attaques contre La Confidentialité

Les attaques contre la confidentialité accéder, intercepter ou divulguer des informations sensibles sans autorisation. Dans le contexte des Smart Grids, des attaques peuvent compromettre les données des consommateurs, les informations sur le réseau et d'autres informations critiques [32].

b) **Types d'attaques contre La Confidentialité** [33]:

- Les attaques par interception de communications, également connues sous le nom d'attaques "man-in-the-middle" (MITM), consistent à intercepter et potentiellement modifier les communications entre deux parties sans leur consentement.
- Accès non autorisé aux bases de données consiste à pénétrer dans des systèmes de stockage de données pour accéder, voler ou altérer des informations sensibles.
- Espionnage industriel implique l'obtention illégale d'informations commerciales confidentielles à des fins de compétition déloyale. Dans les Smart Grids, cela peut inclure des informations sur les stratégies d'exploitation et de gestion de l'énergie.

c) Les mécanismes [33]**:**

- La Cryptographie Utilisation de techniques de chiffrement pour rendre les informations illisibles sans une clé de déchiffrement appropriée.
- La Contrôles d'accès basés sur les rôles (RBAC) Déterminer les droits d'accès aux informations en fonction des rôles des utilisateurs dans l'organisation.

- Les Protocoles de confidentialité des données Garantir que les données personnelles ou sensibles sont protégées pendant la transmission ou le stockage, comme HTTPS pour les communications Web sécurisées.

II.3.2.4 L'Authentification

L'authentification joue un rôle crucial dans la protection des réseaux intelligents contre les intrusions non autorisées. Sa fonction est de confirmer l'identité d'un utilisateur ou d'un système avant d'accorder l'accès aux ressources. Bien que les mots de passe soient couramment utilisés, il est impératif de les compléter par des stratégies telles que l'authentification multifacteur (MFA), qui intègre plusieurs couches de vérification, notamment biométriques. En outre, l'utilisation de cartes à puce et de certificats numériques renforce la sécurité en conservant les informations cryptées. Ces approches contribuent à sécuriser les réseaux intelligents, à protéger les données et à garantir l'intégrité des opérations [31].

a) Les Attaques contre L'Authentification

Les attaques d'authentification visent à contourner les mesures de sécurité établies pour confirmer l'identité des utilisateurs ou des systèmes. Dans le contexte des réseaux intelligents, ces attaques peuvent compromettre la confidentialité, l'intégrité et la disponibilité des données sensibles. Les cybercriminels utilisent différentes techniques pour tirer parti des faiblesses du processus d'authentification, leur permettant d'accéder aux comptes, de voler des informations ou de perturber les services. Ces attaques peuvent cibler les vulnérabilités des mots de passe, les systèmes d'authentification multifactorielle et les protocoles cryptographiques. Par conséquent, les réseaux intelligents doivent mettre en œuvre des mesures de sécurité renforcées, telles que l'authentification multifactorielle et les certificats numériques, pour réduire les risques associés à ces menaces [32].

b) Types d'attaques contre L'Authentification [33]:

- Attaque par force brute, L'assaillant essaie toutes les combinaisons possibles de mots de passe. Les systèmes qui ne limitent pas le nombre de tentatives d'authentification présentent une vulnérabilité.

- Phishing, Les utilisateurs sont induits en erreur par des courriels ou des sites web frauduleux, les incitant à révéler leurs informations d'authentification, ce qui permet à l'assaillant de les récupérer.

- Attaque par dictionnaire, L'assaillant se sert d'une liste de mots de passe courants, visant ceux qui sont souvent employés, afin d'accéder au système plus rapidement qu'avec une attaque par force brute.

- Attaque par rejeu, L'assaillant capte des informations d'authentification durant une session active, puis les utilise ultérieurement pour obtenir un accès non autorisé.

- Attaque sur l'authentification multifactorielle, Bien que cette méthode soit plus sécurisée, elle peut être contournée par l'interception de codes ou par des techniques d'ingénierie sociale, incitant les utilisateurs à divulguer leurs informations.

- Délit de vol de session, L'assaillant s'empare d'un cookie ou d'un jeton de session pour usurper l'identité d'un utilisateur sans nécessiter ses informations d'authentification.

c) Les mécanismes [33]:

- Authentification multifacteur (MFA) : nécessite plusieurs formes de preuve d'identité, telles que des mots de passe, des jetons physiques ou des empreintes digitales biométriques.

- Protocoles d'authentification (par exemple, LDAP, SAML) : permettent la vérification et la gestion des identités sur les réseaux et les applications.

- Gestion des identités et des accès (IAM) : comprend des systèmes de création, de gestion et de révocation des identités et des autorisations dans un environnement informatique.

II.3.2.5 La Non-Répudiation

La non-répudiation est un concept clé en sécurité de l'information, garantissant que les actions effectuées par un utilisateur ou un système sont valides et traçables sans possibilité de falsification. Dans les Smart Grids, ce mécanisme assure l'attribution précise des actions et prévient toute contestation. Les signatures électroniques et les certificats numériques, délivrés par une autorité de

certification (CA), permettent de vérifier l'identité des parties impliquées et l'intégrité des transactions. De plus, une surveillance continue aide à détecter les accès non autorisés, limitant les risques de fraude ou d'abus. L'adoption de techniques de non-répudiation dans les Smart Grids est cruciale pour garantir la transparence des opérations et la sécurité des infrastructures critiques [31].

a) Les Attaques contre La Non-Répudiation

La non-répudiation constitue un principe fondamental de la sécurité, assurant qu'un utilisateur ou un système ne peut pas contester avoir réalisé une action, telle que l'envoi d'un message ou la réalisation d'une transaction. Les attaques visant la non-répudiation tentent de saper cette assurance, permettant ainsi à des individus malintentionnés de renier leur implication dans des actions, même après les avoir exécutées. De telles attaques peuvent engendrer des répercussions significatives dans des systèmes critiques, tels que les réseaux intelligents, en compromettant la confiance et l'intégrité des transactions [32].

b) **Types d'attaques contre La Non-Répudiation** [33]:

- Modification des preuves, L'assaillant altère ou falsifie les éléments de preuve (tels que les journaux ou les signatures numériques) qui assurent l'authenticité des actions réalisées, rendant impossible la démonstration qu'une action a eu lieu.
- Usurpation d'identité, L'assaillant se fait passer pour un autre utilisateur ou système, effectuant des actions en leur nom, ce qui complique la vérification de l'identité réelle de l'auteur.
- Altération des signatures numériques, L'assaillant peut tenter de compromettre les systèmes de signature numérique afin de générer de fausses signatures ou de corrompre les clés privées, ce qui nuit à la fiabilité des signatures électroniques.
- Annulation de certificat, Si un attaquant réussit à annuler un certificat numérique sans raison valable, cela peut conduire à l'invalidation des signatures numériques associées, rendant impossible la vérification de certaines transactions.

c) Les mécanismes [33]**:**

- Signatures numériques Garantissent que l'auteur d'un document ou d'une transaction ne peut pas nier avoir signé ou effectué l'action.

- Journaux et pistes d'audit Enregistrent toutes les actions et transactions effectuées dans un système, permettant de prouver l'exécution d'actions spécifiques par des individus ou des systèmes.
- Accords de niveau de service (SLA) Définitions contractuelles des attentes et des responsabilités pour garantir que les parties ne peuvent pas contester leurs engagements.

1. Conclusion

Dans ce chapitre, nous avons abordé les concepts de base de la sécurité informatique. En comprenant les objectifs de sécurité, les types d'attaques et les mécanismes de protection, nous pouvons améliorer notre capacité à renforcer et à protéger les infrastructures critiques telles que les réseaux intelligents contre les cybermenaces.

Protéger les appareils intelligents contre les attaques est essentiel pour garantir la sécurité énergétique et la protection des données dans un monde de plus en plus interconnecté. L'intégration des technologies de sécurité, le respect des normes internationales, l'utilisation de systèmes d'exploitation sécurisés et la mise en œuvre des meilleures pratiques sont essentiels pour améliorer la résilience des appareils intelligents dans les situations d'urgence.

Ainsi, dans le prochain chapitre, nous approfondirons l’exploration détaillée des IDS pour les réseaux intelligents, car ils font l’objet de cette étude.

Chapitre III : IDS dans les SG

III.1 Introduction

Les réseaux et systèmes informatiques sont exposés à diverses vulnérabilités. Pour contrer ces problèmes de sécurité, une nouvelle approche appelée système de détection d'intrusion a été développée pour agir comme une deuxième ligne de défense et renforcer la sécurité des systèmes informatiques.

Ce chapitre se concentrera sur l'explication de ce concept de détection, en vue de son intégration dans les réseaux électriques intelligents, exposant les différents défis de sécurité dans ce domaine, ainsi que les travaux connexes visant à parvenir à une classification des attaques.

III.2 Définition d’un système d’intrusion :

Selon [34] Un système de détection d'intrusion (ou IDS) est un mécanisme conçu pour repérer les activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte), afin de résoudre les problèmes le plus rapidement possible. Il fournit des informations sur les tentatives d'intrusion réussies ou échouées. En raison de leur utilité pratique, les IDS ont été largement étudiés ces dernières années pour améliorer leur efficacité. Les résultats de ces études ont donné naissance à différentes classes d’IDS qui s’appuient sur différentes techniques de détection, chacune mieux adaptée à un contexte spécifique. Il s'agit notamment des systèmes de détection d'intrusion qui prennent des décisions basées sur les informations trouvées dans les machines hôtes, appelés HIDS, et des systèmes de détection d'intrusion qui prennent des décisions basées uniquement sur les informations circulant dans un réseau, appelés NIDS.

III.3 Les types des IDS :

Les IDS sont des programmes ou des appareils conçus pour surveiller les activités malveillantes d'un réseau ou d'un système informatique, alerter les administrateurs des intrusions potentielles et leur permettre de les contrer [35].

a) Les NIDS :

Le rôle premier d'un réseau IDS, appelé NIDS (Network-based Intrusion Detection System), est d'analyser et d'interpréter les paquets circulant sur le réseau. La mise en œuvre d'un NIDS distant se fait de manière stricte : des capteurs sont placés à des points stratégiques du réseau et génèrent des alertes si des paquets semblent dangereux. Ces alertes sont envoyées vers une console sécurisée, qui les analyse et potentiellement les traite.

On observe fréquemment une structure comprenant une sonde placée à l'extérieur du réseau pour étudier les tentatives d'attaque et une sorte d'interface pour analyser les requêtes ayant transité par le pare-feu. Quelques exemples de NIDS sont : NetRanger, NFR, Snort, DTK, ISS et RealSecure.

b) Les HIDS :

Les systèmes de détection d'intrusion basés sur l'hôte, ou HIDS (Host-based IDS), analysent l'état de fonctionnement des machines sur lesquelles ils sont installés pour détecter les attaques basées sur des démons. Puisqu'ils ne surveillent pas le trafic réseau mais uniquement les activités d'un hôte, ils sont généralement plus précis sur les différents types d'attaques.

Ces IDS utilisent deux types de sources pour fournir des informations sur les activités : les journaux et les pistes d'audit du système d'exploitation. Quelques HIDS connus :

1. Tripwire, Tigre.

2. REGARDEZ, responsable de la sécurité.

3. Dragon Écuyer.

c) IDS hybride :

Les IDS hybrides (NIDS+HIDS) combinent les caractéristiques de plusieurs IDS différents. En pratique, seule la combinaison de NIDS et HIDS est utilisée. Ils permettent de surveiller à la fois le réseau et les points finaux à l'aide d'un seul outil. Les sondes sont placées à des points stratégiques et font office de NIDS et/ou HIDS selon leur localisation. Toutes ces sondes envoient ensuite les alertes à une machine qui centralise et agrège les informations provenant de différentes sources.

III.4 Caractéristiques d'un IDS :

À mesure que la taille des réseaux augmente, il est également important d'être évolutif et robuste, c'est-à-dire qu'un seul composant défaillant ne devrait pas provoquer une panne totale [36].

Les caractéristiques suivantes sont recommandées pour un IDS :

• Fonctionnement continu avec un minimum de supervision.

• Tolérance aux pannes pour récupérer après une panne ou une réinitialisation.

• Résistance à la corruption pour détecter toute modification indésirable.

• Utilisation minimale des ressources du système surveillé.

• Facilement configurable pour une politique de sécurité spécifique.

• Adaptabilité aux changements du système et des utilisateurs.

• Difficulté à se laisser tromper.

III.5 L'architecture d'un IDS :

L'architecture d'un IDS fait référence à la structure globale et à l'organisation des composants qui le constituent, déterminant ainsi la manière dont ces parties interagissent pour atteindre l'objectif commun de détection des intrusions et de protection des systèmes informatiques. Typiquement, un IDS se compose de trois couches principales : la couche de collecte de données, chargée de récupérer les informations pertinentes pour la détection des intrusions, la couche d'analyse, qui interprète les données collectées et applique diverses techniques de détection, telles que la détection basée sur des signatures, des anomalies ou des politiques, et enfin la couche réponse, définissant les actions à entreprendre en cas de détection d'une intrusion [37].

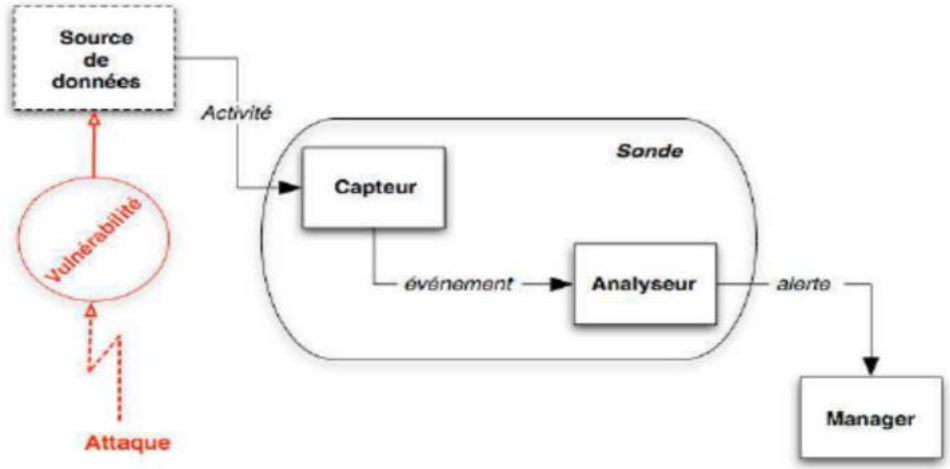


Figure III.1 : L'architecture d'un IDS [38]

III.5.1 Capteur :

Le capteur surveille l'activité du système en utilisant une source de données et transmet à l'analyseur une série d'événements qui informent sur l'évolution de l'état du système. Il est possible que le capteur se contente de transmettre directement ces données brutes, mais généralement un prétraitement est effectué. On peut distinguer traditionnellement trois types de capteurs en fonction des sources de données utilisées pour surveiller l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs.

III.5.2 Analyseur :

Le but de l'analyseur est de vérifier si le flux d'événements provenant du capteur contient des signes d'une activité malveillante. Dans notre étude, un analyseur repose souvent sur des méthodes d'apprentissage automatique (ML), comme les arbres de décision et les techniques de Classification and Regression Trees (CART).

III.5.3 Manager :

Les alertes générées par le capteur sont rassemblées, organisées et présentées à l'opérateur par le manager. Il est possible que le manager soit chargé de prendre la meilleure décision face à l'attaque, qui peut être soit de confiner l'attaque pour limiter ses effets, soit d'éradiquer l'attaque pour tenter de l'arrêter, soit de procéder au recouvrement en restaurant le système dans un état sain, soit de faire un diagnostic pour identifier le problème.

III.6 Mise en place d'un IDS :

La mise en œuvre d'un système de détection d'intrusion (IDS) est une étape essentielle pour améliorer la sécurité d'un réseau ou d'un système informatique. Ce processus implique une série d'actions pour déployer et configurer efficacement un IDS afin de se protéger contre les intrusions et les activités malveillantes [39].

- **Le positionnement d'IDS :**

Il est important de bien choisir les emplacements stratégiques pour l'installation d'un IDS. La figure ci-dessous montre un réseau local et les trois positions possibles pour un IDS.

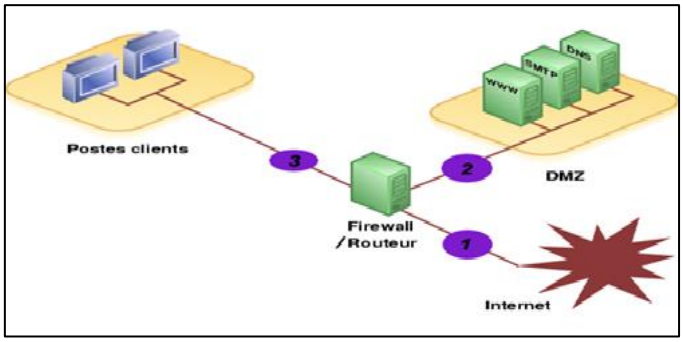


Figure III.2 : Les positions des IDS [40]

- **Position (1)** : A cette position, l'IDS sera capable de détecter toutes les attaques frontales venant de l'extérieur avant le pare-feu. Cela entraînera un grand nombre d'alertes, rendant difficile la visualisation des journaux.

- **Position (2)** : Si l'IDS est positionné sur la DMZ, il sera capable de repérer les attaques qui n'ont pas été bloquées par le pare-feu et qui nécessitent un certain niveau de compétence pour être détectées. Les journaux seront plus clairs à visualiser car les attaques ne seront pas répertoriées.

- Position (3) : Placer l'IDS ici signalera les attaques internes provenant du réseau local de l'entreprise. Il peut être judicieux d'opter pour cette position étant donné que 80 % des attaques viennent de l'intérieur. De plus, si des chevaux de Troie ont infecté le système informatique (suite à une navigation négligente sur Internet), ils peuvent être facilement identifiés et éliminés.

III.7 Mode de fonctionnement

Le mode de fonctionnement d'un IDS (Système de Détection d'Intrusion) repose sur deux aspects fondamentaux : le mode de détection et la réponse apportée en cas de détection d'une intrusion. Ces deux aspects se subdivisent respectivement en détection d'anomalies et reconnaissance de signatures, ainsi qu'en réponse passive et réponse active [41].

III.7 1. Mode de détection

Les IDS utilisent principalement deux méthodes de détection : la détection d'anomalies et la reconnaissance de signatures. Si la reconnaissance de signatures reste la méthode la plus courante sur le marché, les systèmes récents tendent à combiner ces deux approches pour une détection plus efficace des intrusions.

a) Détection d'anomalies :

La détection d'anomalies consiste à identifier des écarts par rapport à un profil de trafic considéré comme normal. Cela nécessite une phase d'apprentissage initiale où l'IDS apprend le comportement habituel des systèmes surveillés. Ensuite, tout écart détecté est considéré comme une anomalie potentielle.

- **Avantages :**

1. Ne nécessite pas de connaissance préalable des attaques, ce qui la rend accessible à un large éventail de situations.
2. Permet la détection des abus de privilèges, renforçant la sécurité du système.
3. Génère des informations utiles pour l'élaboration de signatures, améliorant ainsi les capacités de détection.

- **Inconvénients :**

1. Fort taux de faux positifs, souvent dû à des comportements imprévisibles du réseau et des utilisateurs.
2. Nécessite des ajustements constants pour maintenir le modèle de base à jour, ce qui demande des ressources supplémentaires.
3. Les alarmes génériques peuvent rendre difficile l'identification des menaces réelles, créant une surcharge de travail pour les équipes de sécurité.

b) Reconnaissance de signatures

Cette méthode repose sur la recherche de signatures d'attaques connues au sein du trafic réseau. L'IDS compare les actions observées aux signatures préexistantes dans sa base de données. Cependant, ce type de détection est réactif et limité aux signatures disponibles, nécessitant des mises à jour régulières.

- **Avantages :**

1. Efficace pour détecter des attaques connues avec peu de faux positifs.
2. Permet une réponse rapide et fiable à des outils ou techniques d'attaque spécifiques.
3. Facilite la priorisation des actions correctives en cas d'alerte.

- **Inconvénients :**

1. Ne peut détecter que les attaques pour lesquelles il existe une signature.
2. Nécessite des mises à jour fréquentes pour rester efficace face à de nouvelles attaques.
3. Les signatures génériques, bien que capables de détecter des variantes d'attaques, nécessitent une grande expertise du réseau.

III.7. 2 Réponses actives et passives

Les IDS adoptent deux types de réponses face aux intrusions : la réponse passive et la réponse active. La réponse passive est accessible à tous les systèmes IDS, tandis que la réponse active est implémentée de manière variable selon les modèles [42].

a) Réponse passive

Lorsque l'IDS détecte une intrusion, il enregistre les informations dans un fichier journal pour une analyse ultérieure par l'administrateur. Certains IDS permettent d'enregistrer l'intégralité d'une connexion suspecte, facilitant ainsi l'analyse et la correction des failles de sécurité après coup.

b) Réponse active

La réponse active implique une action immédiate pour stopper l'intrusion, souvent par la reconfiguration automatique d'un pare-feu. Cette reconfiguration permet de bloquer le trafic malveillant en fermant des ports ou en bannissant l'adresse de l'attaquant. Toutefois, cette méthode nécessite un pare-feu compatible avec l'IDS pour effectuer ces actions.

III.8 Synthèse des travaux IDS pour SG :

Article 1 [43] : Détection des cyberattaques dans les réseaux intelligents à l'aide de l'apprentissage supervisé et de la sélection heuristique des caractéristiques (Jacob Sakhnini et al., 2019)

Jacob Sakhnini et al. (2019), ont exploré la détection des attaques par injection de données falsifiées (FDI) dans les réseaux intelligents en utilisant des algorithmes d'apprentissage supervisé et diverses méthodes heuristiques de sélection des caractéristiques. Leur étude s'est concentrée sur trois systèmes IEEE (14-bus, 57-bus et 118-bus) et a évalué la précision de classification de SVM, KNN et ANN avec et sans sélection de caractéristiques. Les résultats montrent que le classificateur SVM a obtenu les meilleures performances globales sur tous les systèmes, avec une précision maximale de 90,59 % après utilisation de l'algorithme génétique (GA). Bien que les méthodes de sélection de caractéristiques aient réduit le nombre de caractéristiques de manière efficace, les ANNs se sont révélées moins performantes dans la détection des attaques FDI, quelles que soient les techniques de sélection des caractéristiques appliquées.

Article 2 [44] : Détection des anomalies dans les réseaux intelligents à l'aide des techniques d'apprentissage automatique (Manikant Panthi, 2020)

Manikant Panthi (2020) a proposé une approche de détection d'anomalies dans les réseaux intelligents en utilisant plusieurs méthodes de classification. L'étude a évalué les performances des classificateurs en termes de précision, rappel et F-mesure sur un jeu de données à trois classes (événements naturels, attaques et absence d'événements). Les résultats montrent que le classificateur Random Forest présente la meilleure capacité de détection des attaques parmi les méthodes testées. Plus précisément, Random Forest a obtenu une précision de 99,2 % pour les non-événements, 92,1 % pour les attaques, et 95,6 % pour les événements naturels. Par comparaison, les méthodes OneR et Naïve Bayes ont montré des performances inférieures, avec des scores de précision particulièrement faibles pour les non-événements et les événements

Article 3 [45] : Système intelligent de détection d'intrusion dans un réseau intelligent utilisant l'intelligence informatique et l'apprentissage automatique (GAN) (Saran et al., 2021)

L'étude de Saran et al. (2021) présente une analyse approfondie des performances des systèmes de détection d'intrusion en utilisant des arbres de décision sur différentes attaques. la classe normale a obtenu une précision de 98,30 %, un rappel de 96,10 % et une mesure F1 de 97,10 %, avec des taux de TP (vrais positifs) et FP (faux positifs) respectivement de 96,10 % et 0,4 %. Les attaques Smurf et Warezclient ont atteint un taux de détection de 100 %, avec un taux de faux positifs respectivement de 0,3 % et 0 %. Le rappel pour les attaques Warezclient et Smurf a également atteint 100 %, avec un score F1 supérieur à 99 % en moyenne pour les deux attaques. En termes de précision, Warezclient a obtenu 99,30 %, et Smurf 98,9 %. Cependant, l'attaque Portsweep a montré un taux de faux positifs plus élevé que les autres, soit environ 1,8 %, avec des scores de précision et de mesure F1 respectivement de 77,20 % et 82,80 %. Pour l'attaque Ipsweep, la précision moyenne, le rappel, la mesure F1 et le taux TP ont atteint 98,50 %, avec un faible taux de faux positifs de 0,2 %. Les attaques Nmap, Back, Teardrop, et Neptune ont également montré des résultats satisfaisants, atteignant en moyenne 93 % en termes de précision, de rappel, et de mesure F1. Ces résultats suggèrent que l'approche basée sur les arbres de décision est particulièrement efficace pour la détection de certaines attaques tout en maintenant un faible taux de faux positifs dans la plupart des cas.

Article 4 [46] : Détection des attaques sur les réseaux intelligents à l'aide de techniques d'apprentissage automatique (Bojja Pranitha, et al 2022)

Bojja Pranitha, et al (2022) ont exploré diverses techniques d'apprentissage automatique pour détecter les attaques dans les réseaux intelligents. Leur étude montre que l'algorithme k-Nearest Neighbors (k-NN) atteint des performances élevées dans les systèmes plus petits, mais son efficacité est compromise par le déséquilibre des données. À l'inverse, les machines à vecteurs de support (SVM) surpassent les autres techniques dans les systèmes à grande échelle, atteignant une précision de 92 %. Le système proposé utilise une distribution probabiliste pour prédire les interruptions potentielles et alerter sur les menaces, permettant des réponses rapides aux anomalies détectées. Les résultats de la simulation indiquent que le système est capable de détecter efficacement les menaces nuisibles avec un taux de détection supérieur à 90 %.

Article 5 [47] : Détection et prévention des attaques par déni de service dans les réseaux intelligents basés sur le cloud (Abdul Razaq, et al 2022)

Abdul Razaq, et al (2022) ont mené des simulations pour examiner les attaques par déni de service (DoS) et leur détection dans les réseaux intelligents basés sur le cloud. L'étude a simulé des attaques DoS en augmentant le flux de paquets pour démontrer la perte de paquets, ce qui représente l'occurrence de DoS lorsque la capacité du système est dépassée, entraînant une indisponibilité du service. Les simulations ont été réalisées sur un réseau où chaque nœud IP correspond à une maison intelligente dans le réseau électrique. Les résultats ont montré que le sous-réseau sécurisé maintenait une communication continue, tandis que le sous-réseau non sécurisé a connu des interruptions et une perte de paquets pendant des intervalles de temps spécifiques (105-350, 500-600 et 800-900 ticks). Un tick représente le plus petit intervalle de temps dans la simulation. Les simulations ont montré que le modèle de panneau solaire était réglé pour produire une production maximale de 5147W, avec des maisons intelligentes ayant une consommation de charge de 0,90% par personne. Le client sécurisé a réussi à envoyer des demandes continues, tandis que le client non sécurisé a rencontré des pertes de paquets significatives en raison de l'attaque DoS.

Article 6 [48] : Sécurité des réseaux intelligents : Une revue systématique (Fifit Alfiah et Novi Rifkhah Prastiwi 2022)

Fifit Alfiah et Novi Rifkhah Prastiwi (2022) ont examiné la cybersécurité des réseaux intelligents dans l'International Journal of Cyber and IT Service Management. Leur étude propose un Système de Détection d'Intrusion Distribué utilisant des techniques comme SVM et AIS. Cette approche a amélioré la détection des données nuisibles de 25% et les chemins de communication sécurisés de 30%. Les auteurs soulignent que les attaques de données modifient les informations des capteurs plutôt que le flux réel d'électricité, et recommandent l'utilisation du cadre NIST pour contrer ces menaces.

Article 7 [49] : Sécurité des réseaux intelligents basée sur la blockchain avec détection de défauts industriels utilisant un réseau de capteurs sans fil et des techniques d'apprentissage profond (Manivel Kandasamy et al. 2023)

Manivel Kandasamy et al. (2023) ont publié une étude dans le Journal of Sensors, Volume 2023, Article ID 3806121. Ils ont comparé les techniques de détection de défauts en utilisant le RMSE (écart quadratique moyen) et le MAP (précision moyenne) pour évaluer les performances des modèles proposés. Leur méthode a atteint un RMSE de 75%, tandis que les méthodes existantes EH_WSN et 6LoWPAN ont obtenu respectivement 89% et 88%. En ce qui concerne le MAP, la technique proposée a obtenu 55%, contre 69% pour EH_WSN et 63% pour 6LoWPAN.

Article 8 [50]: Système intelligent de détection des intrusions dans les réseaux intelligents utilisant l'intelligence computationnelle et l'apprentissage automatique (2021, Suleman Khan, et al)

Dans leur étude publiée dans Transactions on Emerging Télécommunications Technologies en juin 2021, Suleman Khan, et al ont évalué la performance de divers algorithmes de détection des intrusions dans les réseaux intelligents. Les résultats montrent que pour l'algorithme KNN, la précision, le rappel et le score F1 pour la classe normale sont respectivement de 98,89%, 97,60% et 98,20%, tandis que pour la classe d'anomalies, ces valeurs sont de 99,40%, 99,70% et 99,60%. Pour le Random Forest, les scores sont de 98,50% en précision, 99,30% en rappel, et 98,90% en score F1 pour la classe normale, et de 99,80%, 99,60%, et 99,70% pour la classe d'attaques. Les arbres de décision et les réseaux neuronaux ont montré des scores de précision pour la classe normale de 98,50% et 95,40%, avec des rappels et des scores F1 moyens de 99,30% et 98,40%. Pour la classe d'attaques, les scores moyens sont de 97%, 99,60% et 99,50%.

Article9 [51] : Le modèle hybride basé sur CNN et LSTM pour la détection d'intrusions dans les réseaux intelligents (Abdul Hakim Al-Sayari et Muhammad Ilyas, 2024)

Abdul Hakim Al-Sayari et Muhammad Ilyas (2024) ont proposé un modèle hybride de Deep Learning (DL) pour la détection des intrusions dans les réseaux intelligents, en combinant les algorithmes Convolutional Neural Network (CNN) et Long-Short-Term Memory (LSTM). Leur approche utilise un ensemble de données récentes sur les intrusions, spécifiquement axé sur les commandes non autorisées et les attaques par déni de service (DoS). Les résultats expérimentaux montrent que leur méthode CNN-LSTM surpasse les autres algorithmes de Deep Learning en termes de précision, de rappel et de score F1, atteignant un taux de détection élevé de 99,50%.

Article 10[52] : Cadre intégré d'analyse du trafic et de catégorisation des nœuds basé sur l'apprentissage automatique pour la détection et la prévention des intrusions dans les réseaux de capteurs sans fil (WSN) des réseaux intelligents (Tamara Zhukabayeva et al., 2024)

Tamara Zhukabayeva et al. (2024) ont proposé un cadre intégré basé sur l'apprentissage automatique pour la détection et la prévention des intrusions dans les réseaux de capteurs sans fil (WSN) utilisés dans les réseaux intelligents. Ce modèle intègre des techniques d'analyse du trafic et de catégorisation des nœuds pour améliorer la détection des menaces de sécurité. Le cadre utilise les algorithmes d'arbre de décision (DT) et de forêt aléatoire (RF) pour catégoriser le trafic réseau et détecter les anomalies. Les résultats expérimentaux montrent une précision de 95 % avec DT et de 99 % avec RF, confirmant la robustesse du modèle pour protéger les environnements des réseaux intelligents.

III.9 Travaux connexes :

N°	Réf	Année	Auteurs	Titre	Techniques	Algorithmes	Résultats clés
1	[43]	2019	Jacob Sakhnini et al.	IDS dans LES SG	Apprentissage supervisé, sélection de caractéristiques	SVM, KNN, ANN	SVM : 90,59 % de précision après l'utilisation de GA ; ANNs moins performants dans la détection des attaques FDI.
2	[44]	2020	Manikant Panthi	IDS dans LES SG	Apprentissage automatique	Random Forest, OneR, Naïve Bayes	Random Forest : 99,2 % pour les non-événements, 92,1 % pour les attaques, 95,6 % pour les événements naturels.
3	[45]	2021	Saran et al.	IDS dans LES SG	Apprentissage automatique, intelligence artificielle	Arbres de décision	Attaques Smurf et Warezclient : 100 % de détection avec moins de 0,4 % de faux positifs ; Portsweep : faux positifs plus élevés (1,8 %).
4	[46]	2022	Bojja Pranitha et al.	IDS dans LES SG	Apprentissage automatique	k-NN, SVM	k-NN performant sur petits systèmes ; SVM atteint 92 % de précision sur les grands systèmes.
5	[47]	2022	Abdul Razaq et al.	IDS & IPS par DDOS les SG basés sur le cloud	Apprentissage automatique	Non spécifié	Le sous-réseau sécurisé a maintenu la communication continue, tandis que le non-sécurisé a souffert de pertes de paquets pendant les attaques DoS.
6	[48]	2022	Fifit Alfiah et Novi Rifkhah Prastiwi	Sécurité des réseaux intelligents : Une revue systématique	SVM, AIS	SVM, AIS	Augmentation de 25 % dans la détection des données nuisibles et de 30 % dans les chemins de communication sécurisés.
7	[49]	2023	Manivel Kandasamy et al.	Sécurité des SG avec détection de défauts industriels un réseau de capteurs sans fil	Apprentissage profond, blockchain	EH_WSN, 6LoWPAN	RMSE de 75 % ; EH_WSN : 89 % ; MAP de 55 % pour le modèle proposé.
8	[50]	2021	Suleman Khan et al.	IDS DANS SG	Apprentissage automatique, intelligence computationnelle	KNN, Random Forest, Arbres de décision	KNN : 98,89 % de précision, Random Forest : 99,80 % de précision pour les attaques.
9	[51]	2024	Abdul Hakim Al-Sayari et Muhammad Ilyas	IDS DANS SG	Deep Learning, CNN, LSTM	CNN, LSTM	Précision de 99,50 % avec CNN-LSTM, surpassant les autres modèles.
10	[52]	2024	Tamara Zhukabayeva et al.	Cadre intégré d'analyse du trafic et de catégorisation des nœuds pour la (WSN) des SG	Apprentissage automatique	Arbres de décision, Forêt aléatoire	DT : 95 % de précision, RF : 99 % de précision pour la détection d'anomalies.

Tableau III.1 : Comparaison qualitative des travaux reliés

III.10 Conclusion

Dans ce chapitre, nous avons présenté travail. Par la suite, nous avons présenté une synthèse complète de dix articles reliés et récents, qui été comparé dans un tableau selon un ensemble de critères.

La synthèse nous a permet de choisir nos modèles et techniques pour une prédiction plus efficace. Nous avons donc proposé le modèle hybride CNN-LSTM, avec un prétraitement. La conception et les expérimentations du modèle proposé seront données dans le chapitre suivants.

Chapitre IV Conception & implémentation

IV.1 Introduction :

Le quatrième chapitre présente la conception d'un modèle d'IDS pour les SG. Le modèle proposé combine des réseaux de neurones convolutifs (CNN) et des réseaux de neurones récurrents (LSTM) pour fournir une solution efficace aux menaces de sécurité. Nous décrirons dans un premier temps l'architecture générale du système, puis détaillerons les différentes étapes et composants qui composent ce modèle. Il comprend également l'application du modèle proposé. Il affiche diverses options d'implémentation telles que l'environnement de développement, les bibliothèques utilisées et les résultats de la configuration effectuée. Ainsi que les différents tests réalisés et les résultats obtenus grâce à des discussions et comparaisons avec des travaux connexes. Le dataset KDD99 a été utilisé comme base d'apprentissage et de test pour ce projet.

IV.2 Architecture générale du système :

Notre objectif de travail est de réaliser un système intelligent capable de détecter des intrusions dans un réseau de Smart Grid. Ce système utilise une interface graphique (GUI) développée avec Tkinter, permettant de charger des données, d'entraîner un modèle d'apprentissage profond, d'évaluer les résultats, et d'afficher diverses analyses telles que le rapport de classification, la matrice de confusion, et l'exactitude de l'entraînement. Ce modèle de Deep Learning utilisé pour la détection des intrusions est basé sur une architecture hybride combine CNN et LSTM.

Le modèle proposé montre dans la figure suivante :

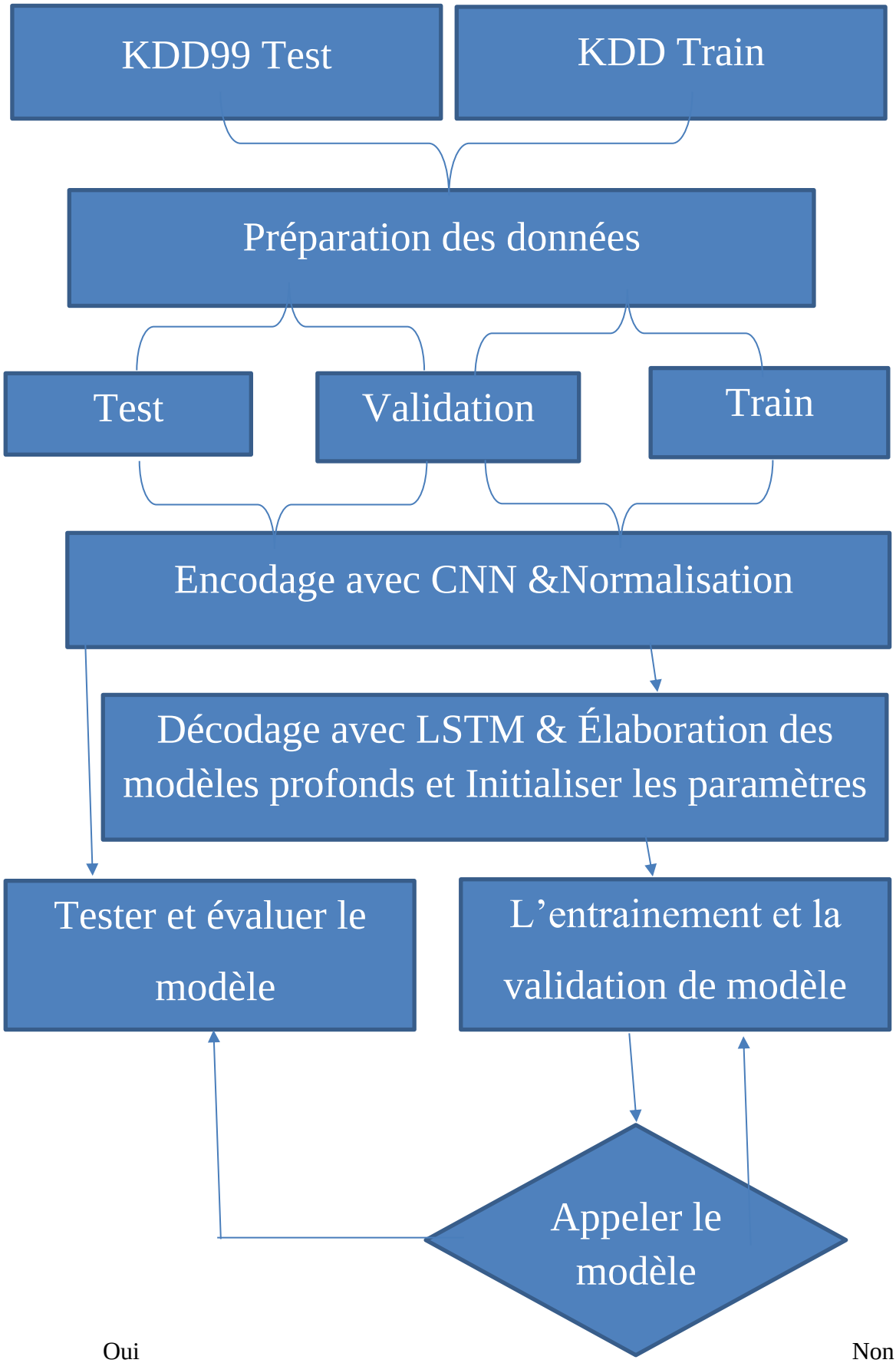


Figure IV.1: architecture du modèle proposé CNN-LSTM.

Ensemble de données :

L'ensemble de données KDD99 est utilisé dans la détection d'intrusion pour le projet de SG. Il est largement connu pour évaluer les IDS grâce à ses journaux de trafic réseau détaillés, y compris les types de protocole, la taille des octets échangés et divers indicateurs d'attaque. Cet ensemble de données couvre à la fois le comportement normal et les attaques simulées, telles que les attaques par déni de service (DoS) et les tentatives de force brute. En intégrant KDD99, nous pouvons tester et améliorer les modèles de détection d'intrusion et améliorer la sécurité du réseau intelligent en évaluant en permanence les performances des algorithmes [53].

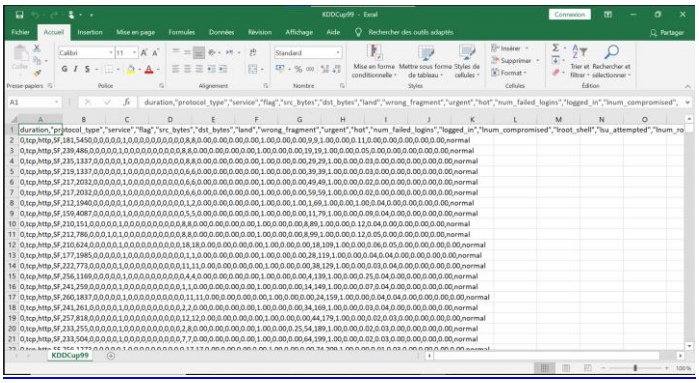


Figure IV.2 : Représentation de la base de Données

➢ **Gestion des données manquantes et normalisation des données :**

Nous utilisons le jeu de données KDD99, qui peut contenir des valeurs manquantes. Les données manquantes sont généralement représentées par des entrées vides dans les fichiers CSV. Pour gérer ces valeurs manquantes, il est crucial de s'assurer que le modèle n'est pas biaisé par des informations incomplètes.

- **Traitement des données manquantes :**

Dans des scénarios réels où des valeurs manquantes sont présentes, on pourrait envisager de compléter ces valeurs avec des statistiques pertinentes, pour éviter ce problème, nous utilisons la moyenne ou la médiane de chaque colonne, ou d'utiliser des techniques d'imputation plus avancées. Cela permettrait d'éviter les biais et les distorsions dans les données qui pourraient affecter les performances du modèle.

- **Normalisation des données :**

Pour préparer les données à l'entraînement du modèle, il est essentiel de normaliser les valeurs numériques afin qu'elles aient une échelle comparable. Dans ce projet, nous utilisons les méthodes

MinMaxScaler pour transformer des valeurs numériques en une plage commune, généralement comprise entre : 0 et 1. Cela permet d'accélérer la formation du modèle et d'améliorer sa convergence. La normalisation garantit que les caractéristiques de différentes échelles n'influencent pas de manière disproportionnée le modèle Deep Learning.

IV.3.1 Phase d'apprentissage :

Après le prétraitement des données, les données sont transmises au modèle proposé pour la formation. Ce modèle est une hybridation d'un réseau neuronal convolutionnel (CNN) et d'un réseau neuronal à mémoire à long terme (LSTM), capturant ainsi à la fois les aspects spatiaux et temporels des données du SG.

Le CNN agit comme un encodeur en extrayant des caractéristiques clés des séquences de données d'entrée. Il se compose de plusieurs couches, dont une couche d'entrée, une couche de convolution et une couche de pooling maximal. La couche de convolution effectue une opération de convolution sur les séquences de données, facilitant l'extraction de caractéristiques significatives. Par la suite, la couche de pooling maximal réduit la dimensionnalité des données et le nombre de paramètres, ce qui optimise l'efficacité de calcul du modèle.

Les résultats du CNN sont ensuite transmis à la section LSTM du modèle, qui agit comme un décodeur. Le LSTM est capable de capturer les dépendances temporelles à long terme dans les séquences de données, ce qui est essentiel pour la détection d'intrusion, où les modèles d'attaque peuvent se développer sur de longues périodes. Le LSTM dispose de mécanismes internes, appelés portes, qui régulent le flux d'informations à travers le réseau, lui permettant de conserver les données pertinentes tout en éliminant les informations superflues.

Une fois le modèle formé, il est capable de faire la différence entre un comportement normal et une activité malveillante au sein du SG. Cette approche hybride exploite les avantages des deux architectures, le CNN pour l'extraction de caractéristiques et le LSTM pour la modélisation temporelle, ce qui donne lieu à un modèle robuste pour la détection des intrusions.

IV.3.2 Prédiction

Après avoir entraîné le modèle hybride CNN-LSTM, celui-ci est utilisé pour faire des prédictions sur les données de test. Ce processus de prédiction consiste à exécuter de nouvelles données de trafic réseau via le modèle pour déterminer si elles reflètent un comportement normal ou une tentative d'intrusion.

Le CNN, ayant acquis la capacité d'extraire des caractéristiques clés des séquences de données pendant la phase d'entraînement, continue d'agir comme un encodeur. Il convertit les séquences de données entrantes en une représentation condensée des caractéristiques les plus significatives. Ces caractéristiques sont ensuite transmises au LSTM, qui examine les séquences, en tenant compte des dépendances temporelles, pour fournir des prédictions précises.

Le LSTM, grâce à ses mécanismes internes de régulation du flux d'informations, analyse les séquences pour détecter des modèles temporels pouvant indiquer une intrusion. En sortie du LSTM, le modèle génère une prédiction binaire, indiquant si la séquence est associée à un comportement normal ou anormal.

Les résultats de prédiction sont comparés aux étiquettes réelles des données de test pour évaluer les performances du modèle. Des indicateurs tels que la précision, le rappel et la courbe ROC peuvent être utilisés pour mesurer l'efficacité de la détection d'intrusion. Ces prédictions sont essentielles pour renforcer la sécurité du réseau intelligent, permettant une réponse rapide et adaptée aux menaces identifiées.

IV.3 Implémentation :

Cette partie présente les outils de développement ainsi que le langage de programmation employés pour la conception et la réalisation du système de détection d'intrusions au sein des SG.

IV.3.1 Langage de Programmation et Bibliothèques :

a) Python :

Au cours des dernières années, Python est devenu le langage de programmation le plus utilisé par les professionnels de l'informatique. Ce choix est dû à la robustesse de Python, à sa large gamme de bibliothèques pour l'apprentissage automatique et la manipulation de données, et à sa facilité d'intégration avec divers outils de visualisation et de traitement de données. Il est devenu une force majeure dans la gestion des infrastructures, l'analyse des données et le développement de logiciels. Avec Python, les développeurs peuvent se concentrer sur l'essence de leur travail, plutôt que sur les détails techniques de sa réalisation. En effet, Python a libéré les développeurs des contraintes imposées par les anciens langages de programmation, rendant le processus de développement de code plus rapide et plus efficace [54].

b) Bibliothèques utilisées

TensorFlow : nous avons utilisé cette bibliothèque pour définir les composants de base de l'architecture CNN-LSTM. Cette bibliothèque est destinée pour l'implémentation des algorithmes d'apprentissage automatique et profond, elle offre aussi une grande flexibilité dans le cadre de l'utilisation pour le développement d'un réseau des neurones [55].

Keras : permet les bibliothèques utilisées avec TensorFlow est Keras, nous avons utilisé cette bibliothèque pour implémenter les couches les différentes couches, les fonctions d'activation et la préparation de la base d'apprentissage [56].

NumPy : nous avons utilisé cette bibliothèque pour adapter les types d'entrée selon la configuration du modèles utilisés, destinée à manipuler des matrices ou tableaux multidimensionnels ainsi que des fonctions mathématiques opérant sur ces tableaux. Nous avons utilisé cette bibliothèque exactement dans le cas de balayage de l'image et l'extraction des fenêtres [57].

Matplotlib : est une bibliothèque du langage de programmation Python destinée à tracer et visualiser des données sous formes de graphiques, nous avons utilisé cette bibliothèque pour visualiser note images sous formes de graphiques [58].

Sklearn : est l'une des bibliothèques les plus utiles pour l'apprentissage automatique en Python. La bibliothèque sklearn contient de nombreux outils efficaces pour l'apprentissage automatique et la modélisation statistique, notamment la classification, la régression, le clustering et la réduction de la dimensionnalité [59].

Tkinter : est une bibliothèque d'interface utilisateur graphique portable (GUI) open source conçue pour être utilisée dans les scripts Python. Tkinter repose sur la bibliothèque Tk, la bibliothèque GUI utilisée par Tcl/Tk et Perl, qui est à son tour implémentée en C. Par conséquent, on peut dire que Tkinter est implémenté en utilisant plusieurs couches [60].

Pandas : Pandas est une bibliothèque logicielle écrite pour le langage de programmation Python pour la manipulation et l'analyse de données. Elle propose notamment des structures de données et des opérations pour la manipulation de tableaux numériques et de séries chronologiques. Il s'agit d'un logiciel libre publié sous la licence BSD à trois clauses [61].

```
import numpy as np
import pandas as pd
from sklearn import preprocessing
from sklearn.preprocessing import StandardScaler
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelBinarizer
import matplotlib.pyplot as plt
import tensorflow as tf
from tensorflow.keras.layers import Dense, LSTM, MaxPooling1D, Dropout, Conv1D
from tensorflow.keras.models import Sequential
```

Figure IV.3 : Importation des Bibliothèques utilisées

IV.3.2 Environnement de Développement :

1) Google Colab : Colaboratory ou « Colab » est un Permet d'écrire et d'exécuter le code Python de son choix par le biais du navigateur. Offert par Google (gratuit), basé sur Jupyter Notebook et destiné à la formation et à la recherche dans l'apprentissage automatique. Cette plateforme permet d'entraîner des modèles de Machine Learning directement dans le Cloud [61], Colab permet :

- D'améliorer les compétences de codage en langage de programmation Python.
- De développer des applications en Deep Learning en utilisant des bibliothèques Python populaires telles que Keras, TensorFlow, PyTorch et OpenCV.
- D'utiliser un environnement de développement (Jupyter Notebook) qui ne nécessite aucune configuration, Mais la fonctionnalité qui distingue Colab des autres services est l'accès à un processeur graphique GPU, totalement gratuit.

2) Anaconda : Anaconda est une distribution scientifique de Python. Permet d'écrire et d'exécuter le code Python de son choix par le biais du navigateur. Offert par anaconda Enterprise (gratuit), utilisé Jupyter Notebook et destiné à la formation et à la recherche dans l'apprentissage automatique [61].

IV.3.3 Environnement matériel :

Le travail d'implémentation a été développé sur un ordinateur ayant les caractéristiques suivantes :

- Intel(R) Core (TM) i7-8650U CPU @ 1.90GHz 2.11 GHz
- Mémoire RAM : 8,00 Go (7,84 Go utilisable).
- Disque dur : 237 Go.
- Windows 10 professionnel, Système d'exploitation 64 bits, processeur x64.

IV.3.4 Implémentation de l'Architecture CNN-LSTM :

L'implémentation de l'architecture CNN-LSTM a été effectuée en plusieurs phases : le modèle a été élaboré en combinant des couches convolutives pour l'extraction des caractéristiques et des couches LSTM pour modéliser les dépendances temporelles présentes dans les données. Par la suite, le modèle a été entraîné, validé et testé sur les données de KDD99.

IV.4 Description de l'application :

IV.4.3 Analyse et discussion des résultats :

Les résultats ci-dessus montre que les performances de notre modèle sont globalement satisfaisantes. En effet, le modèle détecter les intrusions avec un taux de réussite de 99%. De plus, les indicateurs de précision et de rappel sont respectivement d'environ 99% et 99%, ce qui démontre la capacité du modèle à identifier les intrusions avec précision tout en garantissant une détection fiable.

Layer (type)	Output Shape	Param #
conv1d_1 (Conv1D)	(None, 121, 32)	128
max_pooling1d_1 (MaxPooling1D)	(None, 60, 32)	0
lstm_1 (LSTM)	(None, 32)	8,320
dense_1 (Dense)	(None, 1)	33

```
Total params: 8,481 (33.13 KB)
Trainable params: 8,481 (33.13 KB)
Non-trainable params: 0 (0.00 B)
Epoch 1/10
```

Figure IV.4 : Résultat du model

- **Analyse et interprétation des résultats : Suite** à l'entraînement de notre modèle, nous avons observé des résultats prometteurs concernant la précision, le rappel, le score F1 et le taux de fausses alarmes. Cette section présente une analyse approfondie des performances de notre modèle en examinant les indicateurs clés et en explorant leur portée et leur importance.

- **Évaluation globale :**

Évaluation des courbes d'apprentissage :

Les courbes d'apprentissage indiquent que le modèle converge de manière satisfaisante, bien qu'un léger décalage entre la précision d'apprentissage et de validation soit observable. Cela suggère que le modèle n'est pas sur-adapté, mais pourrait bénéficier de techniques de régularisation supplémentaires pour optimiser sa généralisation.

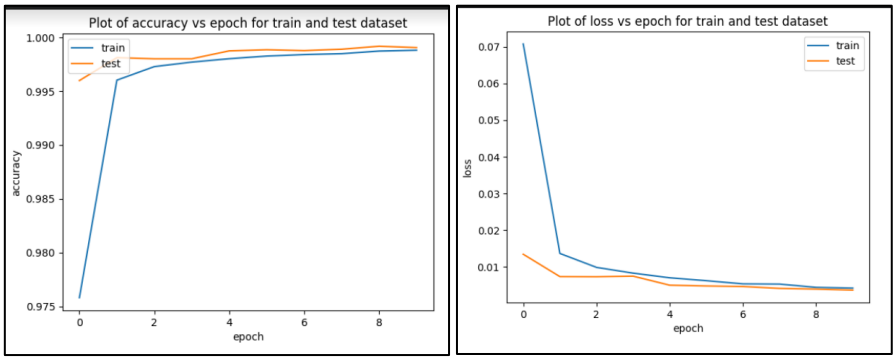


Figure IV.5 : Évaluation des courbes d'apprentissage

- **Analyse de la matrice de confusion :**

L'examen de la matrice de confusion a permis de quantifier les prédictions correctes et incorrectes pour chaque catégorie. Le taux de fausses alarmes est resté inférieur à 12,27 %, ce qui est un indicateur favorable pour un système de détection d'intrusion, car un taux de fausses alarmes élevé pourrait entraîner des conséquences indéables.

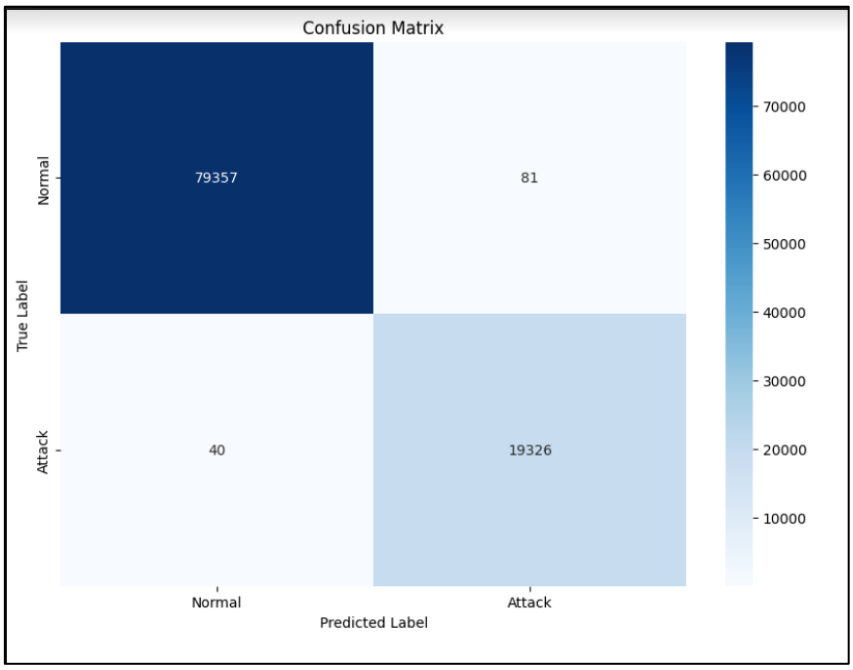


Figure IV.6 : Analyse de la matrice de confusion

IV.4.4 Métriques de performance :

Le modèle proposé est évalué à l'aide des mesures de performance standard suivantes :

- Exactitude (Accuracy) :

Mesure la proportion de prédictions correctes parmi toutes les prédictions faites par le modèle. L'Exactitude est utile lorsque les classes sont équilibrées.

$$\text{Exactitude}=\frac{TP+TN}{TP+TN+FP+FN}$$

- Précision :

Il s'agit du rapport entre les vrais positifs et le nombre total d'occurrences prédites comme positives. Elle est particulièrement importante lorsque le coût des faux positifs est élevé.

$$\text{Précision} =\frac{TP}{TP+FP}$$

- Rappel (Recall)ou sensibilité :

Mesure la capacité du modèle à identifier correctement les exemples positifs parmi les exemples vraiment positifs. Le rappel est crucial lorsque le coût des faux négatifs est élevé.

$$\text{Recall}=\frac{TP}{TP+FN}$$

- F-mesure (F1-score) :

C'est la moyenne harmonique de la précision et du rappel. Elle est utile lorsque l'équilibre entre précision et rappel est nécessaire.

$$\text{F1}=2X\ \frac{Prcision\ X\ Recall}{Prcision+\ Recall}$$

- Matrice de confusion :

Elle fournit un résumé des performances du modèle en termes de vrais positifs, de vrais négatifs, de faux positifs et de faux négatifs. C'est un outil visuel important pour comprendre comment les prédictions du modèle sont distribuées.

Chaque métrique a son importance en fonction du contexte d'application. Dans le cas d'un IDS, un faible taux de faux négatifs (c'est-à-dire des attaques non détectées) est souvent plus critique, ce qui pourrait rendre le rappel ou le F1-score des métriques plus pertinentes que l'exactitude.

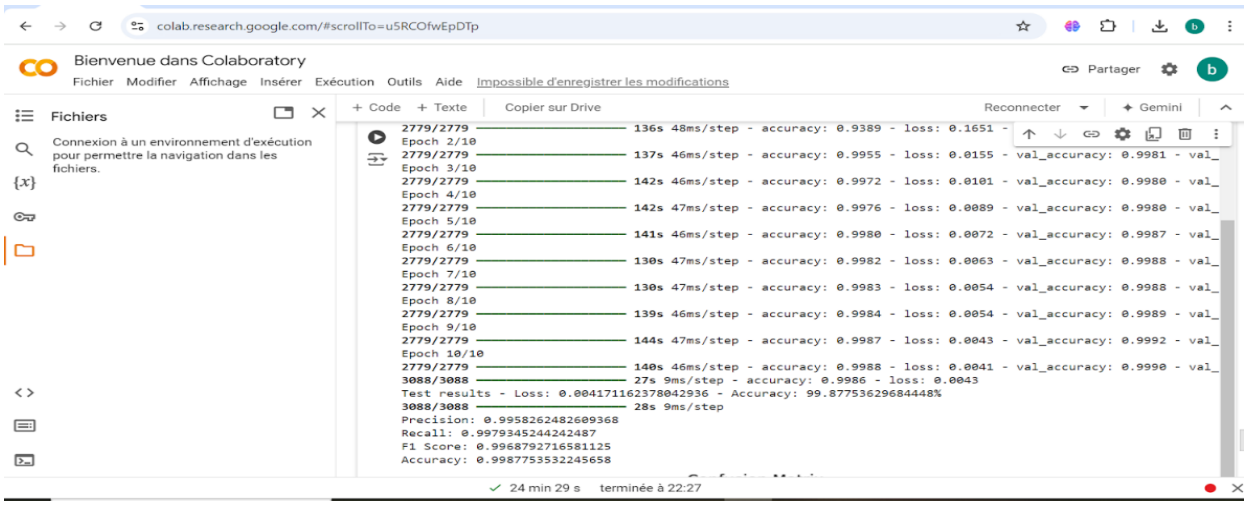


Figure IV.7 : Résultats obtenus

IV.4.5 Comparaison avec d'autres modèles de référence :

Comparaison entre modèles implémentés

Réf	Modèle	Exactitude	Précision	Rappel	F1-score
[43]	SVM	-	90,59 %	-	-
[44]	Random Forest	-	99,2 %	92,1 %	95,6 %
[45]	Arbres de décision	-	99,30 % (Warezclient) / 98,90 % (Smurf)	100 % (Warezclient) / 100 % (Smurf)	99 % (Warezclient) / 99 % (Smurf)
[46]	SVM	92%	-	-	-
[50]	KNN	98,89 %	97,60 % (normal) / 99,40 % (anomalies)	98,20 % (normal) / 99,70 % (anomalies)	-
[50]	Random Forest	99,80 %	99,60 % (anomalies)	99,70 % (anomalies)	-
[51]	CNN-LSTM	99,50 %	-	-	-
[52]	Arbres de décision	95%	-	-	-
[52]	Forêt aléatoire	99%	-	-	-
Modèle Proposé (CNN-LSTM)		99,58%	99,87%	99,79%	99,68%

Tableau IV.1 : Comparaison entre modèles implémentés.

IV.5 Conclusion

Dans ce chapitre, nous présentons en détail les résultats de notre modèle de détection d'intrusion appliqué aux Smart Grids. Après avoir détaillé les différentes étapes de prétraitement des données, nous implémentons et évaluons notre modèle à l'aide de diverses mesures de performance. Les résultats obtenus illustrent l'efficacité de notre approche, qui a surpassé plusieurs modèles de référence présents dans la littérature récente.

De plus, nous avons effectué une comparaison de notre modèle avec d'autres techniques bien établies, en utilisant les mêmes jeux de données. Cette analyse comparative a révélé la supériorité de notre modèle proposé en termes de précision et de robustesse, ce qui renforce la pertinence de notre approche pour les applications de détection d'intrusion dans les Smart Grids.

Les performances de notre modèle mettent en évidence son potentiel pour améliorer la sécurité des Smart Grids. La conclusion générale abordera les perspectives d'amélioration de nos travaux ainsi que les orientations de recherche futures dans le domaine de la détection d'intrusion au sein des systèmes critiques Smart Grid.

Conclusion Générale et Perspectives :

Cette recherche a permis de développer et d'évaluer avec succès un modèle de système de détection d'intrusion (IDS) spécialement adapté aux SG, un domaine où la sécurité est primordiale en raison de la nature sensible des données et des infrastructures critiques impliquées. L'étude a abordé les défis inhérents à la sécurisation des SG en introduisant un modèle qui intègre diverses méthodologies avancées, notamment les réseaux neuronaux convolutionnels (CNN) et les réseaux de mémoire à long terme (LSTM), pour capturer efficacement la dynamique spatio-temporelle des données du réseau.

Les résultats de cette recherche indiquent que le modèle proposé est efficace, démontrant des performances supérieures par rapport aux modèles de référence, comme en témoignent des mesures élevées telles que l'exactitude, la précision, le rappel et le score F1. Cette supériorité a été validée par une analyse comparative complète avec les approches existantes dans la littérature. Les résultats soulignent la capacité du modèle à détecter les anomalies avec précision et fiabilité, ce qui est essentiel pour protéger les infrastructures critiques des réseaux intelligents contre les attaques potentielles.

Bien que le modèle ait montré des résultats prometteurs, il existe plusieurs pistes d'amélioration et d'exploration future. Une amélioration potentielle consiste à renforcer la robustesse grâce à des techniques d'optimisation des hyperparamètres, telles que l'optimisation bayésienne ou les algorithmes génétiques. De plus, l'intégration de techniques d'apprentissage actif pourrait faciliter l'adaptation du modèle aux menaces nouvelles et inconnues, améliorant ainsi ses capacités de détection des attaques zero-day.

L'élargissement des données de test pour inclure divers ensembles de données reflétant des scénarios réels permettrait d'évaluer davantage la généralisabilité du modèle dans divers contextes de réseau intelligent. Une prochaine étape importante consisterait à déployer le modèle dans un environnement de réseau intelligent réel, suivi d'une évaluation de ses performances dans des conditions réelles, ce qui fournirait des informations essentielles sur son efficacité opérationnelle.

Références :

[1] Syed, D., et al (2020). Analyse des Big Data dans les réseaux intelligents : Revue des technologies, techniques et applications. IEEE Access, vol. 8, pp. [1],

[2] Alfiah, F., & Prastiwi, N. R. (2022). Cybersécurité dans la technologie des réseaux intelligents : Une revue systématique. International Journal of Cyber and IT Service Management (IJCITSM), 2(1), avril, p. 48. p-ISSN : 2797-1325, e-ISSN : 2808-554X. Université de Raharja, Indonésie.

[3] Mountassir, F., Mali, R., & Bousmah, M. (2018). Machine Learning au service de la prédiction de la demande d'énergie dans les Smart Grid. Mediterranean Telecommunications Journal, 8(2), 123-130.

[4] Talaei Khoei, T et al (2022). Cybersécurité des réseaux intelligents : attaques, détection, techniques de contremesure et orientations futures. Communications et réseaux, 14, 119-170.

[5] Skrzypczak, A. (2019). Smart Grids. 1ère version, Novembre 2019. ENSICAEN, Bat. F – Bureau 311.

[6] Ye, F et al (2018). Smart Grid Communication Infrastructures : Big Data, Cloud Computing, and Security. First Edition. John Wiley & Sons Ltd.

[7] Fonseca, T., et al. (2022). Flexigy Smart-grid Architecture. In Proceedings of the 11th International Conference on Sensor Networks (SENSORNETS 2022) (pp. 176-183).

[8] Mustafa, M. A. (2015). Smart Grid Security : Protecting Users' Privacy in Smart Grid Applications [Thesis]. The University of Manchester.

[9] Baumeister, T. (2010). Literature Review on Smart Grid Cyber Security. Collaborative Software Development Laboratory, Department of Information and Computer Sciences, University of Hawai, Honolulu, HI.

[10] HADJSAÏD, N., & SABONNADIÈRE, J.-C. (2015). Electricité 21 : Les innovations dans l'approvisionnement électrique. Décembre 2015.

[11] Baig, Z. A., & Amoudi, A.-R. (2013). Une analyse des attaques sur les réseaux intelligents et des contre-mesures. Journal des communications, 8(8), août 2013. Université King Fahd du pétrole et des minéraux, Dhahran 31261, Arabie Saoudite.

[12] Aloul, F. et al. (2012). Sécurité des réseaux intelligents : menaces, vulnérabilités et solutions. Journal international des réseaux intelligents et des énergies propres, 1(1), 1-6.

[13] Berghout, T., et al. (2022). Apprentissage automatique pour la cybersécurité dans les réseaux intelligents : une étude approfondie basée sur un examen des méthodes, des solutions et des perspectives. Energy Reports, 8, 450-473.

[14] Aillerie, Y., et al. (2013, Juin). La Cybersécurité du Smart Grid : Le Déploiement du Smart Grid Nécessite une Nouvelle Approche en Termes de Cybersécurité. Livre Blanc sur la Cybersécurité. Alstom Grid, Intel Corporation, & McAfee. (Version PDF, 6 pages, Français).

[15] Guérard, G. (2014). Optimisation de la diffusion de l'énergie dans les Smart Grids (Thèse de doctorat en Informatique). Université de Versailles-Saint Quentin en Yvelines.

[16] Zheng, T., et al. (2022). Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin.

[17] Abbassi, Y., & Benlahmer, H. (2021). Un aperçu sur la sécurité de l'internet des objets (IOT). Colloque sur les Objets et systèmes Connectés - COC'2021, IUT d'Aix-Marseille, Marseille, France.

[18] Mocanu, S. (2019). Cybersécurité des smart grids. ENSE3/Grenoble-INP, Laboratoire d'Informatique de Grenoble.

[19] Hamdan, A. (2016). Thèse de doctorat en Génie Électrique. Université Grenoble Alpes, École Doctorale Electronique, Electrotechnique, Automatique, Traitement du Signal (EEATS), sous la direction de F. Cadoux et la co-direction de C. Bobineau.

[20] Aye, F. (2009). Intégration des énergies renouvelables pour une politique énergétique durable à Djibouti. Thèse de doctorat, Université Pascal Paoli, France.

[21] Buczak, A.L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[22] Liu, Y, et al (2017). An overview of intrusion detection system : A data mining approach. Journal of Network and Computer Applications, 88, 1-15.

[23] Ahmed, M.et al (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[24] Alfiah, F., & Prastiwi, N. R. (2022). Cybersécurité dans la technologie des réseaux intelligents : une revue systématique. International Journal of Cyber and IT Service Management (IJCITSM), 2(1), avril. p-ISSN : 2797-1325. Université de Raharja, Indonésie.

[25] L. Salvail (2014). "Mécanismes de sécurité des systèmes," 10e cours, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal.

[26] M. Davoodi, R. et al (2020). A Fog-based Approach to Secure Smart Grids Against Data Integrity Attacks. College of Engineering, University of Georgia, Athens, GA 30602, USA.

[27] Wang, W et al (2018). A survey on intrusion detection in smart grid. IEEE Access, 6, 22569-22582.

[28] Aldairi, A., et al (2017). A survey of intrusion detection systems in smart grid communication networks. Journal of Network and Computer Applications, 90, 106-127.

[29] Farooq, M.Oet al (2018). A review of intrusion detection systems in smart grid environments : Issues and solutions. Computers & Electrical Engineering, 65, 283-294.

[30] W. Wang, Z. Lu (2013). "Cybersécurité dans le Smart Grid : Enquête et enjeux," Réseaux informatiques, vol. 57, pp. 1344-1371.

[31 E. Bou-Harb, C. et al (2013). "Communication Security for Smart Grid Distribution Networks," IEEE Communications Magazine, vol. 51, no. 1, pp. 42-49.

[32] T. Docquier (2021). Méthodologies pour l'évaluation de performances d'architectures réseaux smart grids. Thèse de doctorat, Université de Lorraine.

[33] C. Brossollet (2020). Acceptabilité des smart meters - un point de vue usager. Travail de Fin d'Études, Faculté des Sciences appliquées, Master en ingénieur civil architecte, à finalité spécialisée en ingénierie architecturale et urbaine

[34] Liu, X., et al (2021). A Deep Learning-Based Method for Intrusion Detection in Smart Grid. IEEE Transactions on Smart Grid, 12(2), 1562-1570.

[35] Alnajjar, K., et al (2021). Smart grid intrusion detection using deep learning : A survey. Sustainable Energy, Grids and Networks, 26, 100456.

[36] Wu, Z., et al (2021). A novel intrusion detection method for smart grid based ont joint deep learning model. Journal of Electrical Systems and Information Technology, 8(1), 1-11.

[37] Maurras Ulbricht Togbe, et al (2020). Étude comparative des méthodes de détection d'anomalies. HAL Id: hal-02874904. Soumis le 19 juin 2020.

[38] Qingyu Yang, et al (2016). On Optimal PMU Placement-based Defense against Data Integrity Attacks in Smart Grid. IEEE, 1556-6013.

[39] Jianguo Ding, et al (2022). Cybermenaces contre les réseaux intelligents : examen, taxonomie, solutions potentielles et orientations futures. Énergie, vol. 15, no. 18, article 6799.

[40] Ma, Z., et al (2021). An Intrusion Detection System for Smart Grid Based on Machine Learning Algorithm. IEEE Access, 9, 23974-23984.

[41] Alshehri, A. et al(2021). A Deep Learning Approach for Intrusion Detection in Smart Grids. IEEE Access, 9, 42634-42642.

[42] Yeh, J. et al (2021). Deep Learning-Based Anomaly Detection for Smart Grids : A Comprehensive Review. Energies, 14(3), 617.

[43] Jacob Sakhnini, et al. (2019). Détection des cyberattaques dans les réseaux intelligents à l'aide de l'apprentissage supervisé et de la sélection heuristique des caractéristiques. IEEE Access, vol. 7, pp. 1234-1245.

[44] Manikant Panthi (2020). Détection des anomalies dans les réseaux intelligents à l'aide des techniques d'apprentissage automatique. IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 567-574.

[45] Saran, et al. (2021). Système intelligent de détection d'intrusion dans un réseau intelligent utilisant l'intelligence informatique et l'apprentissage automatique (GAN). Journal of Network and Computer Applications, vol. 176, Article 102562.

[46] Bojja Pranitha, et al. (2022). Détection des attaques sur les réseaux intelligents à l'aide de techniques d'apprentissage automatique. International Journal of Electrical Power & Energy Systems, vol. 134, Article 107308.

[47] Abdul Razaq, et al. (2022). Détection et prévention des attaques par déni de service dans les réseaux intelligents basés sur le cloud. IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2345-2356.

[48] Fifit Alfiah & Novi Rifkhah Prastiwi (2022). Sécurité des réseaux intelligents : Une revue systématique. International Journal of Cyber and IT Service Management, vol. 5, no. 2, pp. 89-101.

[49] Manivel Kandasamy, et al. (2023). Sécurité des réseaux intelligents basée sur la blockchain avec détection de défauts industriels utilisant un réseau de capteurs sans fil et des techniques d'apprentissage profond. Journal of Sensors, vol. 2023, Article ID 3806121.

[50] Suleman Khan, et al. (2021). Système intelligent de détection des intrusions dans les réseaux intelligents utilisant l'intelligence computationnelle et l'apprentissage automatique. Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, Article e4132.

[51] Abdul Hakim Al-Sayari & Muhammad Ilyas (2024). Le modèle hybride basé sur CNN et LSTM pour la détection d'intrusions dans les réseaux intelligents. Applied Soft Computing, vol. 136, Article 109202.

[52] Tamara Zhukabayeva, et al. (2024). Cadre intégré d'analyse du trafic et de catégorisation des nœuds basé sur l'apprentissage automatique pour la détection et la prévention des intrusions dans les réseaux de capteurs sans fil (WSN) des réseaux intelligents. IEEE Transactions on Industrial Informatics, vol. 20, no. 3, pp. 1567-1578.

[53] M. Tavallaee, et al (2009) "A detailed analysis of the KDD Cup 99 data set," in *Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009)*, 2009, pp. 1-6.

[54] Simon Yuill et Harry Halpin, *Python*. Copyright (c) 2006.

Webographie

[55]https://www.tensorflow.org/?hl=fr

[56]https://www.Keras.com/about-us

[57]https://numpy.org/

[58]https://matplotlib.org/

[59]https://scikit-learn.org/stable/index.html

[60]https://www.cs.mcgill.ca/~hv/classes/MS/TkinterPres/

[61] https://www.anaconda.com/about-us