UQAC
Université du Québec
à Chicoutimi

# OBSERVATOIRE DES VULNÉRABILITÉS IOT : TEMPS DE REMÉDIATION ET PRÉDICTION DES VULNÉRABILITÉS FUTURES

**PAR ABDERAOUF BOUHALI**

**MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À CHICOUTIMI EN VUE DE L'OBTENTION DU GRADE DE MAÎTRISE ÈS SCIENCES (M. SC.) EN INFORMATIQUE**

**QUÉBEC, CANADA**

## RÉSUMÉ

Ce mémoire de maîtrise s'appuie sur l'exploitation des bases de données publiques CVE, NVD et ZDI pour mener une analyse approfondie des vulnérabilités, avec un accent particulier sur celles affectant les objets connectés (IoT). Trois approches principales ont été proposées : (1) le développement d'un outil d'observation automatisé en Python permettant d'extraire, structurer et analyser les vulnérabilités IOT publiées entre 2019 et 2024, et d'identifier les principales tendances selon le type d'attaque, le niveau de gravité, les produits ou les fournisseurs concernés ; (2) la mise en place d'une méthode d'estimation du temps de remédiation par fournisseur, fondée sur des études existantes et une analyse comparative des métadonnées temporelles, afin d'évaluer leur réactivité face aux vulnérabilités critiques ; (3) une phase expérimentale impliquant plusieurs modèles de machine learning supervisés (XGBoost, MLP, LSTM, BERT) appliqués à un jeu de données structuré, visant à prédire l'apparition probable de vulnérabilités dans les jours suivants pour un produit donné. L'analyse statistique a mis en évidence plusieurs tendances majeures, telles que la prédominance des attaques réseau, la forte exposition des caméras de surveillance et la concentration de failles critiques chez certains fournisseurs. La méthode d'estimation du temps de remédiation a atteint un taux de concordance de 89,81 % avec les données de référence de la Zero Day Initiative, validant ainsi sa fiabilité. En ce qui concerne la prédiction, le modèle XGBoost a obtenu les meilleurs résultats, avec une précision supérieure à 94 %, tandis que les modèles profonds comme LLaMA3, LSTM ou BERT ont montré des performances moindres sur des données temporelles structurées.Les approches proposées et les résultats obtenus ouvrent des perspectives prometteuses pour de futures recherches, notamment sur l'évaluation de la réactivité des fournisseurs et le développement d'outils prédictifs et décisionnels en cybersécurité IoT.

L'IA générative a été utilisée uniquement pour fournir des suggestions ou apporter des corrections mineures (orthographe, grammaire), ainsi que pour clarifier certaines idées dans les paragraphes, afin de garantir une meilleure compréhension du texte.



Mots-clés : Cybersécurité, CVE, NVD, ZDI, IoT, Vulnérabilité, Temps de remédiation, Modèle prédictif, Apprentissage automatique, Apprentissage profond.

## TABLE DES MATIÈRES

## LISTE DES TABLEAUX

## LISTE DES FIGURES

## LISTE DES ABRÉVIATIONS

**IoT** Internet of Things
**IIoT** Industrial Internet of Things
**CVE** Common Vulnerabilities and Exposures
**NVD** National Vulnerability Database
**ZDI** Zero Day Initiative
**CVSS** Common Vulnerability Scoring System
**CWE** Common Weakness Enumeration
**CPE** Common Platform Enumeration
**HTTP** HyperText Transfer Protocol
**MQTT** Message Queuing Telemetry Transport
**SSH** Secure Shell
**API** Application Programming Interface
**REST** Representational State Transfer
**ML** Machine Learning
**LSTM** Long Short-Term Memory
**MLP** Multi-Layer Perceptron
**RNN** Recurrent Neural Network
**biLSTM** Bidirectional Long Short-Term Memory
**GRU** Gated Recurrent Unit
**CNN** Convolutional Neural Network
**XGBoost** Extreme Gradient Boosting
**BERT** Bidirectional Encoder Representations from Transformers
**LLaMA3** Large Language Model Meta AI version 3
**GPT-4o** Generative Pre-trained Transformer version 4o
**MPNet** Masked and Permuted Pre-trained Network
**LLM** Large Language Model
**DoS** Denial of Service
**DDoS** Distributed Denial of Service
**MitM** Man-in-the-Middle
**IA** Intelligence Artificielle
**VMDR** Vulnerability Management, Detection and Response
**UIT** Union Internationale des Télécommunications
**OWASP** Open Web Application Security Project
**T-CVE** Time-Related Vulnerability Lookahead Extension

**OSS** Open Source Software
**OPS** End-of-Support of a Platform or Software
**OODS** Obsolescence of Antivirus or IPS Signatures
**ESW** Expiration of Software License
**SES** Simple Exponential Smoothing
**TES** Triple Exponential Smoothing
**ARIMA** AutoRegressive Integrated Moving Average
**MAE** Mean Absolute Error
**RMSE** Root Mean Square Error
**AFT** Accelerated Failure Time
**ZB** Zettabyte

## DÉDICACE

*À ma mère et à ma soeur. Je vous dédie ce travail en espérant que vous serez toujours fiers de moi. Je dédie également ce travail à tous les membres de la famille, pour leurs encouragements, soutiens, affectation et confiance pour continuer mes études. Au professeur Fehmi Jaafar, qui m'a donné confiance et espoir, et qui m'a soutenu durant toutes mes recherches. À tous ceux qui de près ou de loin ont contribué de quelques manières à la réalisation de ce document. Qu'ALLAH leur accorde la santé, prospérité et leur gratifie de sa miséricorde.*

## REMERCIEMENTS

Tout d'abord, je remercie Dieu de m'avoir accordé la force, la volonté et la patience nécessaires pour mener à bien ce projet.

Je souhaite remercier chaleureusement mon directeur de mémoire, Monsieur Fehmi Jaafar, pour son encadrement rigoureux, sa disponibilité et ses conseils précieux tout au long de ce travail. Son expertise et ses retours pertinents ont grandement contribué à l'orientation et à la qualité de cette recherche.

Mes remerciements s'adressent également à l'ensemble du corps professoral du département de mathématiques et d'informatique de l'Université du Québec à Chicoutimi, pour la richesse des enseignements dispensés et l'environnement stimulant offert au fil de ma formation.

Je tiens aussi à exprimer toute ma gratitude envers ma famille, pour son soutien indéfectible, sa patience et ses encouragements constants tout au long de mon parcours académique. Un merci particulier à ma mère et à ma sœur pour leur présence, leurs soutien et leur encouragement tout au long de ce travail.

À toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire, je vous adresse mes plus sincères remerciements.

# AVANT-PROPOS

Cela fait plus d'un an que j'ai décidé d'entamer mon parcours de maîtrise, après près de cinq ans d'expérience dans le domaine du développement logiciel. Depuis le début de ma carrière, j'ai développé une véritable passion pour la sécurité informatique. En tant que développeur, j'ai eu l'occasion d'interagir avec différents types d'objets connectés, tels que les caméras de surveillance, les casques ou les smartphones. Cela m'a permis de mieux comprendre les défis spécifiques liés à ce domaine émergent qu'est l'Internet des objets (IoT). Cependant, malgré cette curiosité, mes connaissances restaient insuffisantes pour identifier pleinement les menaces spécifiques à ces appareils et gérer efficacement les risques qui y sont associés.

C'est ce qui m'a motivé à entamer un parcours universitaire axé sur la recherche, afin d'acquérir de nouvelles connaissances, notamment dans le domaine de l'IoT, de mieux comprendre ses tendances actuelles et d'identifier des solutions pertinentes, notamment pour la création d'outils complets en cybersécurité.Avec mon directeur de recherche, nous avons conçu un outil complet d'analyse automatisée des vulnérabilités, intégrant des fonctionnalités avancées encore inexistantes à ce jour, notamment la détection d'objets connectés au sein d'une large gamme de produits, la classification des fournisseurs selon leur temps de réponse, ainsi que des modèles prédictifs des vulnérabilités futures.

Je suis très satisfait des résultats obtenus, d'autant plus que nous proposons des solutions inédites dans ce domaine. Ce travail ouvre ainsi de nouvelles perspectives pour les futurs chercheurs qui souhaitent approfondir ces problématiques.Dans le cadre de ce mémoire, un article présentant les principaux résultats a été soumis à **IEEE Transactions on Computers**, revue internationale de référence considérée comme l'une des meilleures dans le domaine de l'informatique [1]. L'article a été retenu pour révision et est actuellement en cours d'évaluation par les pairs.

# CHAPITRE I

# INTRODUCTION

## 1.1 CONTEXTE

L'Internet des objets (IoT) est un écosystème complexe d'objets connectés, capables d'échanger des données via des réseaux filaires ou sans fil, dans le but de fournir des services aux humains comme aux machines. Son développement s'est accéléré au cours de la dernière décennie, porté par l'adoption croissante dans de nombreux secteurs [2]. En 2024, le nombre d'objets IoT actifs dans le monde est estimé à 23,1 milliards, contre seulement 9,2 milliards en 2021, soit une croissance de plus de 150 % en seulement trois ans. Selon IoT Analytics [3], ce chiffre pourrait atteindre 40 milliards d'ici 2030 . Cette prolifération massive d'objets connectés engendre une production exponentielle de données, issues de sources variées telles que les dispositifs médicaux, les capteurs industriels, les systèmes domotiques ou les infrastructures critiques. Selon les prévisions [3], le volume de données généré par l'IoT devrait dépasser 100 zettaoctets par an dès 2025, contre seulement 4,4 ZB pour l'ensemble du trafic Internet mondial en 2020 [4]. La croissance du volume de données à caractère sensible, qu'elles soient d'ordre personnel, étatique, industriel ou financier, accentue les défis en matière de cybersécurité, de protection de la vie privée et de gouvernance de l'information. Malgré leur adoption massive, les objets connectés présentent des limitations structurelles qui en font des cibles privilégiées pour les cyberattaques. La faible puissance de calcul, la capacité mémoire restreinte et l'autonomie énergétique limitée empêchent l'intégration de mécanismes de sécurité avancés [5]. De plus, l'hétérogénéité des plateformes matérielles et logicielles, combinée à l'absence de normes universelles, complique la gestion des correctifs de sécurité [6]. Ces failles systémiques exposent les dispositifs à divers types d'attaques, telles que l'écoute

passive, le détournement de commande, le déni de service (DoS), ou encore l'injection de code malveillant. Dans les environnements critiques, ces vulnérabilités peuvent engendrer des conséquences graves, tant sur le plan opérationnel que sur celui de la confidentialité des données [7]. Le rôle des fabricants est déterminant dans la sécurisation des objets connectés. La fiabilité d'un dispositif IoT dépend en grande partie de la capacité de son fabricant à réagir rapidement et efficacement à l'identification d'une vulnérabilité affectant ses produits. Cette réactivité comprend la détection de la menace, l'analyse de son impact, le développement d'un correctif adéquat, ainsi que la diffusion rapide d'une mise à jour de sécurité auprès des utilisateurs. Le temps de réponse, ou délai de remédiation, défini comme l'intervalle entre la découverte d'une faille et la publication de son correctif, constitue un indicateur clé de la maturité en cybersécurité d'un fournisseur, en particulier pour les équipements déployés dans des environnements critiques. L'étude [8] a montré que ce délai varie considérablement selon les fabricants : certains mettent plusieurs mois à corriger des vulnérabilités pourtant critiques, tandis que d'autres, mieux structurés, s'appuient sur des programmes de divulgation responsable pour accélérer ce processus.

Les vulnérabilités affectant les objets connectés sont généralement rendues publiques après la publication d'un correctif par le fabricant. Parmi les principales bases de données utilisées pour leur référencement figurent le Common Vulnerabilities and Exposures (CVE) et la National Vulnerability Database (NVD), considérées comme des standards par la communauté de la cybersécurité [9]. Ces bases permettent d'identifier les vulnérabilités associées à un produit, d'analyser leur fréquence, leur gravité, ainsi que les vecteurs d'attaque impliqués. En complément, des plateformes spécialisées comme la Zero Day Initiative (ZDI) fournissent des informations souvent absentes des bases de données publiques, notamment la date de détection initiale d'une vulnérabilité par un chercheur ou par le fournisseur. Cependant, le volume considérable et la grande diversité des produits répertoriés dans les référentiels publics incluant des

logiciels, du matériel, ainsi que des systèmes d'exploitation compliquent fortement l'extraction ciblée des vulnérabilités propres aux objets connectés. Ce défi est accentué par l'ambiguïté entourant la définition des objets connectés : l'identification des dispositifs IoT nécessite souvent une analyse approfondie de leurs fiches techniques pour confirmer qu'ils répondent aux critères d'un dispositif IoT [10]. Pour automatiser ce filtrage, des solutions exploitant l'intelligence artificielle capables d'interpréter des sources en ligne en temps réel s'avèrent efficaces. Cependant, leur mise en œuvre à grande échelle demeure coûteuse, notamment pour des tâches récurrentes de classification et d'extraction. De nombreux outils de cybersécurité actuels, tels que Tenable Nessus, Qualys VMDR ou Rapid7 InsightVM [5], s'appuient fortement sur des bases publiques pour orienter leurs processus décisionnels et alimenter leurs systèmes de détection [11]. Bien que ces référentiels fournissent des données précieuses sur les vulnérabilités connues, leur nature réactive et leur manque d'uniformité limitent leur efficacité pour anticiper les menaces émergentes. C'est dans ce contexte que l'intégration de l'intelligence artificielle (IA) dans les solutions de cybersécurité devient primordiale pour permettre une défense proactive [12]. Cette mutation est d'autant plus urgente que les attaquants exploitent eux aussi l'IA pour automatiser plusieurs phases critiques d'une attaque : reconnaissance des cibles, identification de vulnérabilités dans des systèmes obsolètes ou mal configurés, ou encore génération de logiciels malveillants polymorphes capables d'échapper aux antivirus traditionnels [13]. Ces outils abaissent considérablement la barrière technique, permettant à des acteurs peu qualifiés de mener des attaques sophistiquées à moindre effort. Face à cette asymétrie, les spécialistes en sécurité doivent mobiliser des modèles d'apprentissage automatique pour anticiper les vulnérabilités à partir de données historiques, identifier des comportements anormaux et réagir de manière autonome aux incidents. Toutefois, la prédiction des vulnérabilités reste encore sous-exploitée dans les solutions commerciales, en raison des limites d'accès aux données, du manque d'explicabilité des modèles et de la difficulté d'intégration dans les infrastructures critiques. Du côté des défenseurs, les outils d'intelli-

gence artificielle sont principalement déployés autour de trois axes stratégiques : la détection d'anomalies comportementales, la réponse automatisée aux incidents, et la prédiction des vulnérabilités [12]. Parmi ces axes, la prédiction reste à ce jour le volet le moins exploité dans les solutions commerciales de cybersécurité, comme le confirment plusieurs analyses récentes sur l'usage industriel de l'IA en sécurité informatique. Cette sous-exploitation s'explique par plusieurs facteurs [14]. D'une part, les données disponibles dans les bases publiques telles que CVE ou NVD sont souvent hétérogènes, déséquilibrées ou incomplètes, ce qui complique l'entraînement de modèles fiables [15]. D'autre part, la temporalité des événements, le manque de standardisation des descripteurs techniques, et la difficulté à établir des corrélations robustes entre vulnérabilités passées et futures limitent les performances des approches prédictives. De plus, les fournisseurs n'intègrent que rarement des mécanismes de collecte et de structuration des données orientées prédiction, freinant ainsi le développement d'outils généralisables à grande échelle. Cette situation crée un vide méthodologique et technologique que ce mémoire ambitionne de combler à travers une solution basée sur l'apprentissage supervisé.

Dans le cadre de ce projet de recherche, nous concentrons nos efforts sur le développement d'un outil décisionnel de cybersécurité intégrant des fonctionnalités avancées, qui ne sont pas encore proposées par les solutions commerciales actuelles. Ce développement s'appuie sur une méthodologie rigoureuse, articulée autour de trois axes principaux :

**Identification automatisée des objets connectés :** La première composante consiste à concevoir un système automatisé capable d'extraire, à partir d'une vaste gamme de produits référencés dans les bases Common Vulnerabilities and Exposures (CVE) et National Vulnerability Database (NVD), ceux qui correspondent à la définition stricte d'un objet connecté . L'objectif est de générer des statistiques précises sur ces dispositifs, d'identifier les tendances récentes en matière de vulnérabilités, et d'offrir une visualisation claire des produits les plus exposés.

**Calcul du temps de remédiation par fournisseur :** Le second axe propose une méthode innovante pour calculer le temps de remédiation, défini comme l'intervalle entre la détection initiale d'une vulnérabilité et sa correction publique. Ce paramètre, encore rarement exploité dans les outils actuels, constitue un indicateur précieux pour évaluer la réactivité des fabricants. Il peut influencer les décisions d'achat ou de déploiement de technologies, notamment dans des environnements sensibles.

**Prédiction des vulnérabilités futures :** Le troisième axe vise à exploiter les données structurées issues des deux bases publiques CVE et NVD pour entraîner divers modèles d'apprentissage automatique. Cette étape a pour objectif d'évaluer et de comparer les performances de plusieurs algorithmes, notamment des modèles de classification et d'apprentissage profond, dans la prédiction à court terme de vulnérabilités associées à des produits spécifiques. L'analyse comparative permettra d'identifier le modèle le plus performant en vue de son intégration ultérieure dans des systèmes de cybersécurité à capacité prédictive, renforçant ainsi les mécanismes de défense proactive.

## 1.2 MOTIVATION

Les statistiques liées aux objets connectés jouent un rôle crucial pour quantifier leur impact, démontrer leur valeur ajoutée, identifier les besoins en sécurité, et orienter les décisions d'adoption, de conception ou de renforcement des dispositifs IoT, tant dans les environnements industriels que grand public [16]. À ce jour, il n'existe aucun outil fournissant de manière centralisée des statistiques officielles sur le volume annuel de vulnérabilités (CVE) affectant spécifiquement les objets connectés [17]. Pourtant, de nombreux rapports professionnels et études techniques alertent sur l'augmentation continue des failles IoT signalées dans les bases CVE et NVD, une tendance directement liée à la croissance exponentielle du marché des objets connectés [18]. Une étude menée par Dam et al [14] met en évidence

l'importance de l'intelligence artificielle dans la prédiction à court terme des vulnérabilités, soulignant son potentiel pour anticiper les menaces avant leur exploitation. Toutefois, elle insiste également sur les nombreux défis associés à cette approche, notamment la qualité et l'hétérogénéité des données issues des bases publiques, les difficultés liées à l'entraînement de modèles fiables, ainsi que la nécessité de concevoir des algorithmes capables de s'adapter à l'évolution rapide du paysage des menaces. Plusieurs types d'apprentissage peuvent être envisagés à partir des jeux de données disponibles. Toutefois, le choix du modèle revêt une importance cruciale, notamment dans les cas où les données présentent une dimension temporelle (incluant des dates) ou lorsque la tâche de prédiction porte sur des chaînes textuelles. En effet, l'adéquation entre la nature des données et l'architecture du modèle a un impact direct sur la qualité de l'apprentissage et la performance prédictive du système. Selon l'étude [14], la majorité des fabricants d'objets connectés s'efforcent de réagir rapidement aux vulnérabilités affectant leurs produits, en déployant notamment des mises à jour logicielles ou d'autres mécanismes correctifs. Cette réactivité ne répond pas uniquement à des impératifs techniques, mais relève également d'une stratégie de gestion d'image, visant à maintenir la confiance des utilisateurs et des partenaires industriels. Dans un contexte où la sécurité devient un critère différenciateur sur le marché de l'IoT, cette capacité à corriger rapidement les failles constitue un avantage concurrentiel significatif. Cependant, l'absence d'indicateurs de performance unifiés et d'outils d'évaluation normalisés entrave toute tentative de comparaison rigoureuse entre les fournisseurs [19]. De plus, les fabricants ne publient pas systématiquement les délais entre la détection d'une faille et sa correction, limitant ainsi la transparence et rendant difficile l'évaluation de leur maturité en cybersécurité. Cette opacité représente un frein pour les décideurs qui souhaitent baser leurs choix technologiques sur des critères de fiabilité et de sécurité vérifiables [20]. À cela s'ajoute la pression croissante des régulateurs et des marchés, qui exigent de plus en plus la traçabilité et la preuve d'une gestion proactive des vulnérabilités, notamment dans les secteurs critiques.

## 1.3 OBJECTIFS

L'objectif principal de ce projet de recherche est de proposer des solutions méthodologiques et techniques pour combler les lacunes identifiées dans les outils de cybersécurité actuels. En s'appuyant exclusivement sur les ressources publiques disponibles, notamment les bases de données CVE et NVD, ce projet vise à concevoir un prototype fonctionnel d'un outil décisionnel de cybersécurité intégrant des fonctionnalités encore absentes des solutions commerciales. L'ambition est de démontrer qu'il est possible, à partir d'une approche rigoureuse et reproductible, de tirer pleinement parti de ces référentiels pour automatiser des tâches essentielles telles que l'identification des objets connectés vulnérables, l'estimation du temps de remédiation par fournisseur, et la prédiction à court terme de nouvelles vulnérabilités. Ce travail s'inscrit dans une perspective de recherche appliquée, visant à poser les bases d'un système proactif, accessible, et fondé sur des données ouvertes, en réponse aux limites méthodologiques identifiées dans les études récentes. Il convient toutefois de souligner que plusieurs travaux antérieurs ont déjà exploré certaines de ces problématiques, notamment dans le cadre de la classification des vulnérabilités ou de la détection d'attaques réseau. Toutefois, la majorité de ces approches restent limitées à des contextes spécifiques, reposent sur des jeux de données propriétaires ou ne tiennent pas compte des contraintes d'automatisation. Notre démarche se distingue par sa volonté d'unifier, dans un même outil, plusieurs fonctionnalités critiques tout en s'appuyant uniquement sur des sources ouvertes, afin de favoriser la reproductibilité, la transparence scientifique et une application à grande échelle. Ce projet de recherche répond à trois questions principales :

1. **Quelles sont les principales tendances en matière de vulnérabilités affectant les dispositifs IoT ?**

Nous proposons une approche permettant d'identifier automatiquement les produits relevant de l'écosystème IoT à partir de l'ensemble des dispositifs référencés dans les bases CVE

et NVD. À partir de cette classification, nous analysons les vulnérabilités associées à ces produits, signalées entre 2019 et 2024, afin d'identifier les principales tendances [21], en nous concentrant sur les vecteurs d'attaque, les niveaux de gravité, les types de vulnérabilités, ainsi que les fournisseurs les plus impactés. Parallèlement, une analyse globale des vulnérabilités tous produits confondus est menée à des fins informationnelles, afin de dégager les tendances générales affectant l'ensemble du paysage de la cybersécurité[21].

2. **Dans quelle mesure les données issues des bases CVE peuvent-elles être exploitées pour estimer le délai de remédiation des fournisseurs en fonction de la gravité des vulnérabilités ?**

Cette question vise à évaluer la faisabilité d'une estimation automatisée du temps de remédiation moyen par fournisseur, en combinant les métadonnées disponibles dans les bases CVE et NVD avec des informations complémentaires extraites de sources ouvertes (avis de sécurité, rapports techniques, publications spécialisées) [22]. L'objectif est de quantifier la réactivité des fabricants face aux vulnérabilités selon leur niveau de criticité, et d'identifier les écarts de performance entre fournisseurs.

3. **Quels sont les modèles d'apprentissage supervisé les plus adaptés pour prédire l'apparition de vulnérabilités à court terme à partir des données historiques issues des bases CVE ?**

Cette question vise à évaluer la capacité des algorithmes d'apprentissage supervisé à anticiper l'émergence de nouvelles vulnérabilités sur un horizon temporel restreint, en exploitant des jeux de données structurées [21] dérivées des bases publiques CVE et NVD. Pour ce faire, plusieurs modèles sont considérés, allant des approches classiques (régression logistique [23], forêts aléatoires [24], XGBoost [25]) aux méthodes plus avancées, incluant les réseaux neuronaux profonds ((LSTM [26], MLP [27]) et les architectures basées sur le langage naturel (BERT [28]). Ces modèles sont entraînés sur des descripteurs techniques et temporels issus

des historiques CVE, puis comparés selon des critères de performance (précision, rappel, F1-score) afin d'identifier celui offrant la meilleure capacité de prédiction future.

En résumé, ce projet de recherche vise à proposer des approches méthodologiques et techniques innovantes pour combler les lacunes identifiées dans les outils de cybersécurité actuels, en s'appuyant exclusivement sur des ressources publiques ouvertes. L'objectif est de concevoir une première version fonctionnelle d'un outil décisionnel intégrant des fonctionnalités avancées, encore absentes des solutions commerciales existantes.

Ce projet s'articule autour de trois axes complémentaires :

— L'extraction automatisée des objets connectés vulnérables, accompagnée d'une analyse approfondie des tendances en matière de vecteurs d'attaque, de gravité et de typologie des vulnérabilités.

— L'estimation du temps de remédiation par fournisseur, en tant qu'indicateur clé de leur réactivité face aux failles de sécurité.

— La prédiction à court terme de l'apparition de vulnérabilités spécifiques à un produit, à l'aide de modèles d'apprentissage supervisé.

Ce travail se distingue par son approche unifiée, transparente et reproductible, démontrant qu'il est possible de produire des résultats concrets et exploitables à partir de données ouvertes. Il constitue ainsi une première étape vers le développement d'outils de cybersécurité proactifs, évolutifs et scientifiquement fondés.

## 1.4 CONTEXTE DE LA RECHERCHE

Dans le domaine de la cybersécurité, les approches actuelles reposent largement sur des analyses quantitatives et statistiques pour renforcer la protection des systèmes d'information. Comme le soulignent [29], « l'analyse à grande échelle des vulnérabilités logicielles, en exploi-

tant des bases publiques telles que CVE et NVD, permet d'identifier des tendances critiques dans la durée de correction des failles, offrant ainsi aux équipes de sécurité une connaissance approfondie des risques » . La plupart des outils du marché proposent des tableaux de bord synthétiques permettant aux spécialistes de disposer d'une vision panoramique de leur périmètre de sécurité, favorisant une meilleure priorisation des actions correctives. Cependant, dans le contexte de l'Internet des Objets, la sécurité représente un défi majeur, intrinsèquement lié aux caractéristiques propres des dispositifs. Comme l'indiquent [30], « la grande hétérogénéité des équipements, la faible puissance de calcul, ainsi que l'absence de standards normalisés rendent les solutions traditionnelles de cybersécurité difficiles à appliquer dans ce domaine » . De plus, la fréquence élevée des vulnérabilités détectées sur les objets connectés, souvent insuffisamment documentées dans les bases publiques, complique l'évaluation objective de leur sécurité.

Pour pallier ces limites, des méthodes d'analyse dynamique du comportement des dispositifs IoT ont émergé. Par exemple, [31] proposent des solutions fondées sur la surveillance en temps réel des dispositifs, permettant d'identifier automatiquement des comportements inhabituels, des fuites de données potentielles ou des activités malveillantes non détectées par les outils statiques. Cependant, ces approches restent encore peu intégrées dans des outils consolidés offrant des statistiques fines et contextualisées par produit ou par fournisseur. De plus, comme le mentionnent [32], « la réactivité des fournisseurs dans la gestion et la correction des vulnérabilités est un paramètre clé dans l'évaluation opérationnelle de la sécurité des systèmes IoT. Or, les données disponibles sont dispersées et rarement agrégées de manière structurée pour faciliter ces analyses » . Cette lacune met en lumière le besoin croissant d'outils centralisés capables non seulement d'exploiter les bases CVE et NVD, mais aussi de compléter ces données par des informations issues de sources ouvertes, tels que rapports techniques et avis de sécurité spécialisés. Ainsi, le développement d'une plateforme automatisée pour :

— extraire automatiquement les produits IoT et analyser leurs tendances,

— évaluer la rapidité de remédiation des vulnérabilités selon les fournisseurs,

— prédire l'apparition potentielle de nouvelles vulnérabilités.

constitue une avancée significative pour combler ces lacunes. Cette perspective rejoint les conclusions de [33] qui insistent sur l'importance de « coupler des outils analytiques avancés avec une approche proactive de gestion des vulnérabilités afin d'anticiper les menaces et de limiter les surfaces d'attaque dans les infrastructures IoT » . Une telle solution contribue non seulement à renforcer la protection des objets connectés, mais aussi à améliorer la prise de décision des professionnels de la cybersécurité, en fournissant des indicateurs fiables et exploitables pour une meilleure anticipation des risques.

## 1.5 CONTRIBUTION

Les projets de recherche jouent un rôle essentiel dans l'avancement des connaissances et la résolution de problèmes complexes. Leurs contributions se manifestent à plusieurs niveaux, tant sur le plan académique que pratique [34]. Ce projet vise à explorer et à développer des approches innovantes pour renforcer la sécurité des systèmes IoT, alliant rigueur théorique et applicabilité opérationnelle. Les contributions majeures de ce projet sont les suivantes :

1. La réalisation d'une revue approfondie de la littérature portant sur les solutions existantes et les mécanismes décisionnels en cybersécurité, afin d'identifier les meilleures pratiques et les lacunes méthodologiques.
2. L'élaboration d'une démarche méthodologique dédiée à l'extraction et à l'analyse des vulnérabilités spécifiques aux systèmes IoT, intégrant des techniques issues des récentes avancées scientifiques.

3. La proposition d'une méthode inspirée d'études existantes pour l'estimation du temps de remédiation des vulnérabilités par fournisseur, offrant ainsi un indicateur inédit de réactivité dans l'écosystème IoT.
4. La comparaison systématique de différents modèles prédictifs pour déterminer celui le plus adapté à la prévision à court terme des vulnérabilités sur des familles de produits donnés, avec validation empirique.

Ainsi, ce projet vise à combler plusieurs lacunes identifiées dans la littérature, tout en mettant à la disposition des chercheurs en cybersécurité un premier prototype fonctionnel d'outil d'aide à la décision, constituant une version initiale améliorée et opérationnelle, susceptible d'être perfectionnée dans de futurs travaux.

## 1.6 ORGANISATION DU DOCUMENT

Ce document est divisé en six chapitres. Ce chapitre d'introduction montre l'état actuel de la sécurité des objets connectés, expose la motivation et les objectifs de la recherche, le cadre d'étude et met en évidence les contributions proposées. Le deuxième chapitre expose les notions de base nécessaires à la compréhension de notre recherche. Le troisième chapitre propose une revue de la littérature, en présentant l'état de l'art sur la sécurité IoT selon les trois volets de recherche abordés et en examinant les travaux connexes. Le quatrième chapitre couvre la démarche au niveau de la méthodologie incluant la collecte, le nettoyage et la structuration des données, ainsi que les stratégies d'extraction des produits IoT et de construction du jeu de données final. Le cinquième chapitre présente les résultats obtenus en lien avec les trois questions de recherche. Enfin, le sixième chapitre résumera le projet de recherche et les contributions apportées dans l'extraction, la prédiction des vulnérabilités IoT et le calcul du temps de remédiation, ainsi que les pistes futures de recherche.

# CHAPITRE II

# FONDEMENTS THÉORIQUES

Ce chapitre établit le cadre conceptuel et technique de l'étude. Elle introduit d'abord l'Internet des Objets (IoT), en présentant ses principes fondamentaux, les caractéristiques des dispositifs connectés et leurs principaux domaines d'application. Elle aborde ensuite les référentiels publics de vulnérabilités, qui constituent les principales sources de données exploitées pour l'identification, l'analyse et la gestion des failles de sécurité. L'objectif est d'offrir une compréhension globale du contexte dans lequel s'inscrit notre étude sur la cybersécurité et la prédiction des vulnérabilités dans l'écosystème IoT.

## 2.1 INTERNET DES OBJETS (IOT)

L'internet des objets (IoT) est « un réseau mondial constitué d'objets physiques équipés de dispositifs électroniques, qui communiquent entre eux ou avec l'humain, afin de traiter des données contextuelles et d'automatiser des processus.» [35]. L'IoT peut se définir aussi comme étant « une infrastructure dynamique qui connecte des objets physiques à l'Internet, proposant des services basés sur la collecte et l'exploitation continue de données, tout en garantissant l'interopérabilité, la sécurité et la confidentialité [36]. »

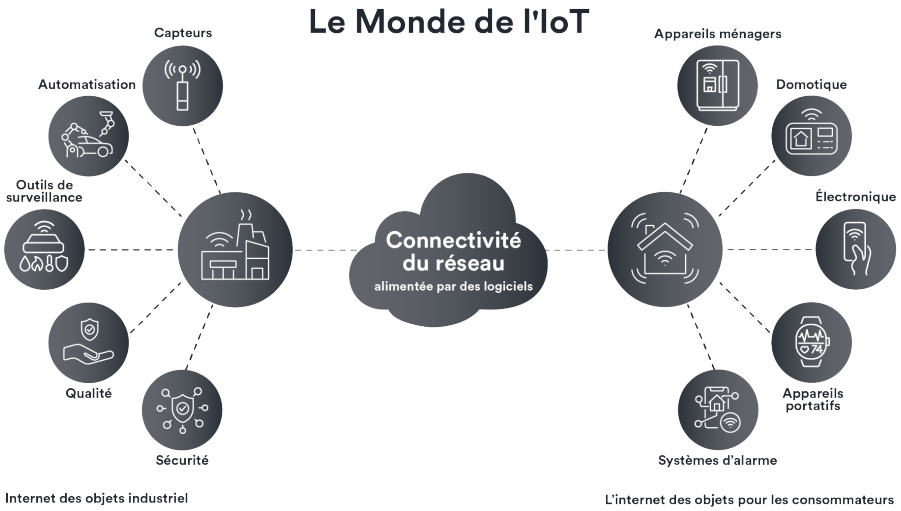


**FIGURE 2.1 : Le monde de l'Internet des objets (IoT)**

Parmi les nombreuses définitions du concept IoT, celle de l'Union internationale des télécommunications (UIT) est considérée comme la plus pertinente pour notre travail de recherche, qui définit l'IoT comme suit : « L'Internet des objets (IoT) est un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques, afin de récupérer, stocker, transférer et traiter sans discontinuité les données liées à ces objets, entre les mondes physiques et virtuels [37]». Dans cette perspective, l'étude repose sur l'analyse des dispositifs qui le composent et des contextes dans lesquels ils sont déployés. Les points suivants présentent d'abord les spécificités des dispositifs IoT, puis les principaux domaines d'application de l'IoT.

1. **Spécificités des dispositifs IoT :** Comme le mettent en évidence les différentes définitions de l'Internet des Objets (IoT), ce concept désigne un réseau formé d'objets connectés, qui en constituent les éléments fondamentaux. Ces dispositifs, appelés également objets physiques ou dispositifs IoT, peuvent être définis comme suit : « Un objet connecté (dispositif IoT) est un dispositif électronique embarqué, autonome ou semi-

autonome, qui intègre un ou plusieurs capteurs/actionneurs, une capacité de traitement locale et des interfaces de communication, lui permettant de percevoir son environnement, de traiter des informations et de les transmettre à d'autres systèmes via des réseaux filaires ou sans fil [38]. » À partir de cette définition, on peut distinguer un simple produit matériel d'un véritable objet connecté en considérant plusieurs caractéristiques essentielles. Un dispositif IoT doit être capable d'interagir avec son environnement via des capteurs et/ou des actionneurs, disposer d'une capacité de traitement embarquée assurant une certaine autonomie, et présenter une connectivité réseau, filaire ou sans fil, pour échanger des données avec d'autres systèmes. Enfin, il doit pouvoir communiquer avec une plateforme logicielle ou un service distant, permettant la supervision, la commande ou l'analyse des informations collectées. Ces critères ont servi de repères tout au long de notre étude pour identifier et classer rigoureusement les objets connectés.

2. **Domaines d'application de l'IoT :** L'Internet des objets connaît une expansion rapide dans de nombreux secteurs, grâce à sa capacité à collecter, transmettre et traiter des données en temps réel. Dans le domaine de la santé, les dispositifs médicaux connectés permettent le suivi à distance des patients, l'autosurveillance des constantes vitales, et la gestion intelligente des traitements [5]. L'IoT joue également un rôle clé dans l'industrie (IIoT), en facilitant la maintenance prédictive, l'optimisation des processus de production et l'automatisation des lignes d'assemblage. Les villes intelligentes exploitent ces technologies pour améliorer la gestion du trafic, surveiller la qualité de l'air ou optimiser l'éclairage public. Dans le secteur agricole, l'IoT contribue à une agriculture de précision, grâce à des capteurs de sol, des systèmes d'irrigation automatisés et des dispositifs de suivi du bétail [20]. À l'échelle domestique, les maisons intelligentes intègrent des thermostats, caméras de sécurité et appareils électroménagers connectés pour accroître confort et sécurité.

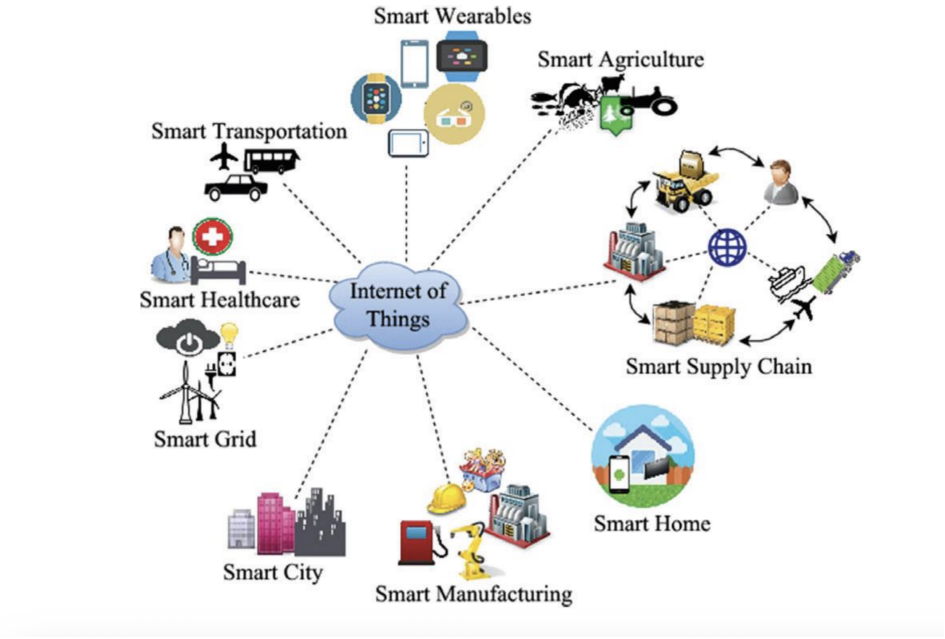


**FIGURE 2.2 : Domaines d'application de l'Internet des objets [39]**

L'IoT est également central dans la logistique, l'environnement, et les réseaux énergétiques intelligents, où il permet un suivi en temps réel, une meilleure efficacité opérationnelle et une gestion optimisée des ressources. Ces multiples domaines illustrent l'impact transversal de l'IoT sur les infrastructures modernes et la transformation numérique des systèmes physiques [39].

## 2.2 CONCEPTS FONDAMENTAUX EN CYBERSÉCURITÉ

La cybersécurité regroupe l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la protection des systèmes d'information et des utilisateurs dans le cyberespace contre les actes portant atteinte à la disponibilité, à l'intégrité ou à la confidentialité des données, des services ou des systèmes [40]. Dans le contexte des systèmes connectés, l'analyse de la cybersécurité s'appuie sur plusieurs notions fondamentales per-

mettant de caractériser les risques et les mécanismes de protection. Les concepts présentés ci-dessous sont utilisés tout au long de cette étude.

**Vulnérabilité IoT :** Les vulnérabilités IoT désignent les failles de sécurité présentes dans les composants matériels, logiciels ou dans la configuration des objets connectés, qui peuvent être exploitées par des attaquants pour compromettre la confidentialité, l'intégrité ou la disponibilité du dispositif ou de son environnement. Elles peuvent entraîner des interruptions de service, des fuites de données, des manipulations physiques ou logiques, voire des prises de contrôle à distance [41].

**Surface d'attaque :** La surface d'attaque d'un système informatique regroupe tous les points d'exposition et d'interaction exploitables par des attaquants, qu'il s'agisse d'interfaces physiques, de protocoles réseau, de composants logiciels ou de plateformes cloud. Dans le contexte IoT, cette surface s'accroît notamment du fait des nombreuses interfaces sans fil, des API et des firmwares présents sur les objets connectés, ce qui augmente significativement le risque d'accès non autorisé ou de compromission du système [19].

**Temps de remédiation :** Le temps de remédiation des vulnérabilités désigne le délai écoulé entre la détection d'une vulnérabilité et la mise en œuvre effective d'une action corrective, telle qu'un correctif logiciel (patch), une mise à jour de sécurité ou une reconfiguration du système. Ce délai constitue un indicateur clé de performance permettant d'évaluer la capacité d'une organisation à réagir de manière rapide et appropriée face aux menaces informatiques [42].

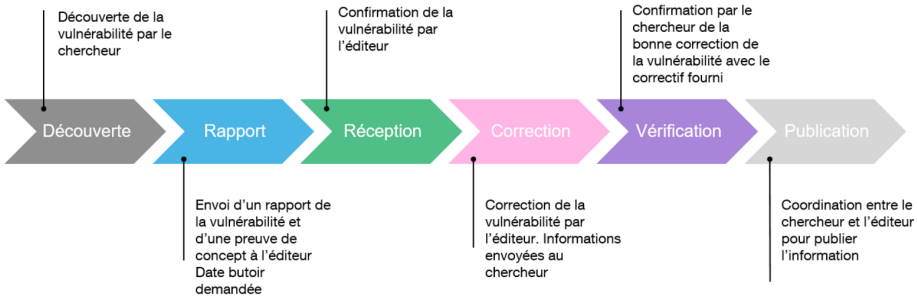


**FIGURE 2.3 : Processus de divulgation responsable d'une vulnérabilité**

Dans un système d'information, ce temps se mesure généralement en heures ou en jours et reflète directement la vitesse de réponse opérationnelle de l'entité concernée. Réduire ce temps est essentiel pour limiter la période durant laquelle le système demeure vulnérable aux attaques potentielles, et ainsi minimiser les risques d'exploitation [42]. Le temps de remédiation peut principalement servir comme un critère d'évaluation de l'efficacité d'un acteur. Un temps de réponse court témoigne d'une bonne anticipation, de processus de gestion des vulnérabilités bien établis, ainsi que d'une capacité d'intervention rapide dans un contexte de cybersécurité dynamique.

**Scores CVSS (Common Vulnerability Scoring System) :** Le CVSS est un système de notation standardisé utilisé pour évaluer la gravité des vulnérabilités informatiques. Il permet d'apprécier la criticité d'une faille selon des critères objectifs et mesurables, offrant ainsi aux acteurs concernés la possibilité de prioriser les correctifs et de gérer les risques de manière plus efficace et cohérente.

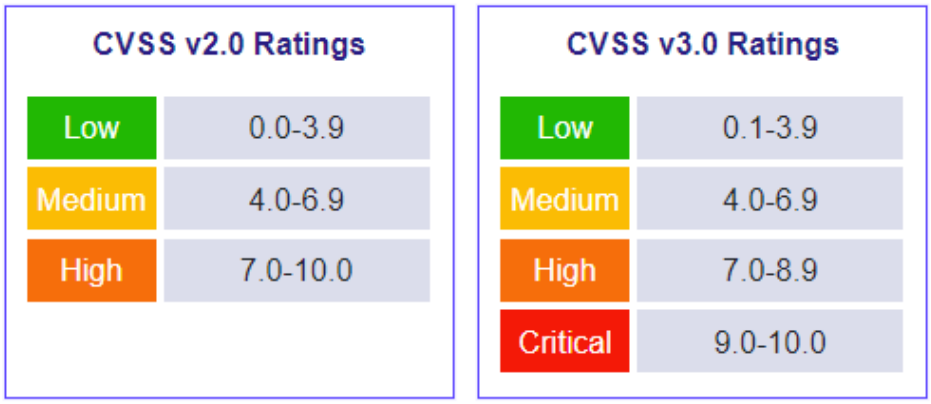


**FIGURE 2.4 : Échelle de gravité CVSS v2.0 et v3.0**

Jusqu'à présent, deux versions principales du score ont été proposées : le CVSS v2 et le CVSS v3, ce dernier apportant une meilleure précision et étant le plus largement utilisé. La figure 2.4 illustre l'échelle de gravité du CVSS en fonction des différentes versions disponibles [43].

## 2.3 RÉFÉRENTIELS PUBLICS DE VULNÉRABILITÉS

Afin de comprendre le domaine d'application de cette étude, cette section vise à présenter les concepts fondamentaux ainsi que les principales sources de données exploitées. Elle décrit les référentiels publics de vulnérabilités utilisés tout au long de ce travail, qui constituent des ressources essentielles pour l'identification, l'analyse et la gestion des failles de sécurité. Cette présentation permet de mieux situer les choix méthodologiques adoptés et d'en faciliter l'interprétation des résultats obtenus.

### 2.3.1 COMMON VULNERABILITIES AND EXPOSURES - CVE

La base de données CVE est un répertoire public et normalisé qui recense les vulnérabilités et expositions de sécurité informatique connues et divulguées. Chaque vulnérabilité

référencée dans cette base possède un identifiant unique, appelé CVE ID (par exemple : CVE-2025-12345), accompagné d'une description claire permettant aux organisations et aux spécialistes en cybersécurité de communiquer efficacement et de gérer les risques liés à ces failles. Maintenue par la MITRE Corporation, la base CVE agit comme un dictionnaire centralisé des vulnérabilités, facilitant notamment l'interopérabilité entre différents outils et bases de données de sécurité, comme NVD aux États-Unis. Elle inclut des informations telles que la description de la vulnérabilité, les systèmes affectés et d'autres métadonnées essentielles pour l'évaluation et la remédiation [44]. Chaque vulnérabilité répertoriée dans la base CVE est associée à des mécanismes d'évaluation de sa gravité (CVSS), implémentés au sein de référentiels complémentaires. Cette structuration normalisée permet une identification cohérente des vulnérabilités et constitue le socle de nombreuses analyses et processus de gestion des risques en cybersécurité.

### 2.3.2 NATIONAL VULNERABILITY DATABASE - NVD

Le National Vulnerability Database (NVD) est la base de données gouvernementale américaine qui centralise et enrichit les vulnérabilités référencées par le CVE grâce à des notations standardisées et des métadonnées complémentaires. Maintenue par le NIST, elle facilite l'automatisation, la mesure de sécurité et la gestion efficace des vulnérabilités dans les systèmes d'information, offrant ainsi un référentiel fiable pour la communauté sécurité. [43]

### 2.3.3 ZERO DAY INITIATIVE - ZDI

La Zero Day Initiative (ZDI) est un programme international de divulgation responsable des vulnérabilités, fondé en 2005 par TippingPoint et aujourd'hui opéré par Trend Micro. Son objectif principal est d'encourager le signalement confidentiel des vulnérabilités zero-day

(failles inconnues non encore corrigées) en offrant des récompenses financières aux chercheurs en cybersécurité. La ZDI agit comme un intermédiaire de confiance : elle acquiert les informations sur les failles auprès des chercheurs, vérifie leur authenticité dans ses laboratoires, puis notifie de façon confidentielle le fournisseur concerné pour qu'il puisse développer un correctif avant toute publication. En parallèle, le chercheur garde l'anonymat et bénéficie d'une protection juridique et financière fournie par la plateforme [45]. Ce qui distingue la Zero Day Initiative (ZDI) des autres programmes, selon sa documentation officielle et les analyses techniques, est la publication d'un bulletin technique enrichi, diffusé après la correction d'une vulnérabilité, et comprenant des métadonnées détaillées telles que la date de détection initiale, la date de notification au fournisseur, ainsi que la date de publication ou de correction de la faille [45]. Ces informations sont rendues publiques afin de renforcer la transparence et de faciliter la compréhension du cycle de remédiation par la communauté.

Dans le cadre du calcul du temps de remédiation d'un fournisseur, en comparaison avec d'autres acteurs, la ZDI constitue une source particulièrement fiable, notamment grâce à la précision de ses dates. Elle représente ainsi une référence importante, juste après les bulletins officiels émis directement par les fabricants.

## 2.4 PRINCIPES DE L'APPRENTISSAGE AUTOMATIQUE

Un algorithme d'apprentissage automatique (machine learning) est un processus informatique qui permet à une machine d'apprendre automatiquement à effectuer une tâche spécifique en analysant des données, sans être explicitement programmée pour chaque étape. En s'appuyant sur des techniques statistiques, probabilistes et mathématiques, ces algorithmes identifient des motifs récurrents, détectent des relations complexes et construisent des modèles prédictifs ou décisionnels [46]. L'objectif est de permettre au système d'améliorer ses performances au fil du temps grâce à l'expérience acquise à partir des données. L'apprentissage

d'un modèle suit plusieurs étapes clés (comme montre la figure 2.5) : collecte des données, prétraitement, séparation en jeu d'entraînement et de test, entraînement du modèle, évaluation de ses performances, puis déploiement. Chaque étape contribue à améliorer la précision du modèle et sa capacité à généraliser sur de nouvelles données. La qualité du jeu de données est essentielle au succès de l'ensemble du processus.

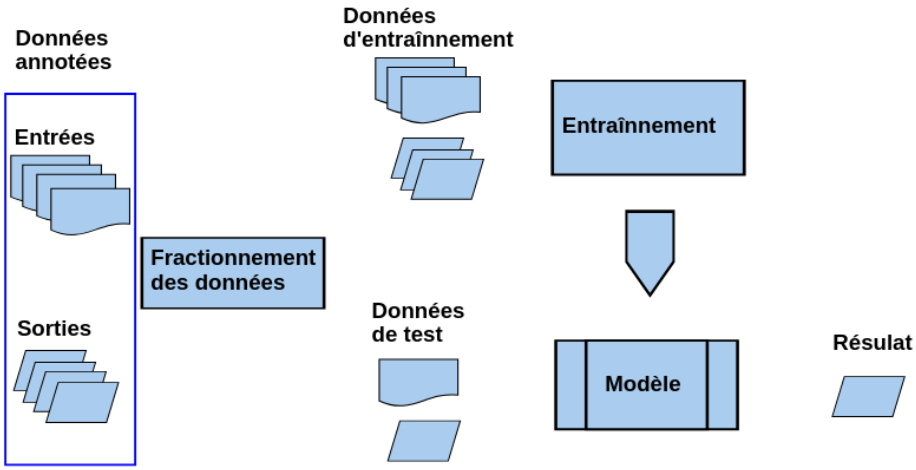


**FIGURE 2.5 : Principales étapes de l'entraînement d'un modèle de machine learning**

Plusieurs types d'algorithmes d'apprentissage automatique sont présentés dans la littérature, chacun étant conçu pour répondre à des besoins spécifiques en fonction de la nature des données et des objectifs d'analyse. Chaque modèle nécessite un jeu de données adapté à sa logique d'apprentissage, sa complexité et son domaine d'application. Ces algorithmes sont généralement classés en trois grandes catégories :

— **Apprentissage supervisé :** repose sur l'utilisation de jeux de données étiquetés, pour lesquels la sortie attendue est connue. L'objectif de l'algorithme est d'apprendre la relation entre les variables d'entrée et les étiquettes, afin de prédire ou de classer de nouvelles données. Cette approche est largement utilisée pour des tâches de classification,

de régression ou de détection, notamment lorsque des données annotées sont disponibles. Cette catégorie inclut également les approches semi-supervisées, qui combinent un nombre limité de données étiquetées avec un volume plus important de données non étiquetées, permettant d'améliorer les performances des modèles lorsque l'annotation manuelle est coûteuse ou difficile à obtenir.

— **Apprentissage non supervisé :** s'applique à des données non étiquetées et vise à extraire des informations pertinentes sans connaissance préalable des résultats attendus. L'algorithme cherche à identifier des structures, des regroupements ou des régularités au sein des données, ce qui permet de révéler des comportements ou des profils similaires. Ce type d'apprentissage est couramment utilisé pour l'exploration de données, la segmentation, la détection d'anomalies ou la réduction de dimension, notamment en phase d'analyse exploratoire.

— **Apprentissage par renforcement :** repose sur l'interaction entre un agent et un environnement dynamique. L'algorithme apprend à prendre des décisions en fonction de récompenses ou de pénalités associées à ses actions, dans le but de maximiser un gain cumulatif à long terme. Cette approche est particulièrement adaptée aux systèmes séquentiels et autonomes, où les décisions prises influencent les états futurs du système, comme dans la robotique, les systèmes adaptatifs ou certains mécanismes de sécurité automatisée.

L'apprentissage supervisé est particulièrement adapté à notre problématique, car il permet de construire des modèles prédictifs fiables et interprétables. Les données exploitées, issues de référentiels publics de vulnérabilités, sont déjà étiquetées, ce qui facilite l'apprentissage et permet une évaluation objective des performances à l'aide de métriques telles que la précision, le rappel ou le score F1. Cette approche constitue ainsi une base méthodologique pertinente pour l'analyse et la prédiction des vulnérabilités dans les systèmes IoT.

## 2.5 MÉTRIQUES D'ÉVALUATION EN APPRENTISSAGE AUTOMATIQUE

Pour les problèmes de classification, l'évaluation des modèles consiste à comparer les classes prédites aux classes réelles. Cette comparaison est résumée dans la matrice de confusion, qui sert à calculer les principales métriques d'évaluation. Les notations utilisées dans les formules de calcul sont définies comme suit :

— $VP$ : prédictions positives correctes

— $FP$ : prédictions positives incorrectes

— $VN$ : prédictions négatives correctes

— $FN$ : prédictions négatives incorrectes

À partir de ces notations, il est possible d'analyser les performances globales du modèle, notamment lorsque les classes sont déséquilibrées. Parmi les métriques les plus couramment utilisées figurent l'exactitude, la précision, le rappel et le score F1. Chacune de ces métriques met en évidence un aspect spécifique de la performance du modèle, rendant leur utilisation complémentaire nécessaire pour une évaluation fiable et rigoureuse. Afin de mieux comprendre ces métriques, elles sont définies comme suit :

— **Exactitude :** L'exactitude mesure la proportion de prédictions correctement classées par le modèle parmi l'ensemble des observations. Elle fournit une vision globale des performances, mais peut être peu représentative lorsque les classes sont déséquilibrées.

$$\text{Exactitude} = \frac{VP + VN}{VP + VN + FP + FN}$$

— **Précision :** La précision évalue la fiabilité des prédictions positives du modèle. Elle correspond à la proportion des instances correctement prédites comme positives parmi

toutes celles prédites positives.

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

— **Rappel :** Le rappel mesure la capacité du modèle à identifier correctement les instances positives. Il indique la proportion des instances réellement positives qui ont été correctement détectées par le modèle.

$$\text{Rappel} = \frac{VP}{VP + FN}$$

— **Score F1 :** Le score F1 est la moyenne harmonique de la précision et du rappel. Il permet d'obtenir un compromis équilibré entre ces deux métriques et est particulièrement adapté aux jeux de données présentant un déséquilibre entre les classes.

$$\text{Score F1} = 2 \times \frac{\text{Précision} \times \text{Rappel}}{\text{Précision} + \text{Rappel}}$$

Dans le cadre de cette étude, l'évaluation des modèles de classification s'appuie sur ces métriques, dont l'analyse conjointe permet une appréciation rigoureuse des performances, en particulier lorsque les classes sont déséquilibrées.

# CHAPITRE III
# REVUE DE LA LITTÉRATURE

## 3.1 ORGANISATION DE LA REVUE DE LITTÉRATURE

Cette revue de littérature est organisée en trois parties principales :

**État de l'art sur l'analyse des vulnérabilités :** Cette partie présente les principales sources de données sur les vulnérabilités, notamment CVE et NVD, ainsi que les travaux qui les exploitent pour étudier l'évolution des failles de sécurité. Elle aborde également les outils de détection et d'analyse proposés dans la littérature, les études sur les tendances dans l'IoT, ainsi que les méthodes d'identification des produits liés à l'IoT.

**État de l'art sur le délai de remédiation :** Cette partie s'intéresse aux travaux portant sur l'estimation et l'amélioration des temps de correction des vulnérabilités. Elle traite des problématiques liées à l'identification des dates de découverte et de correction, ainsi que des solutions et défis associés à l'extraction fiable de ces informations.

**Application de l'intelligence artificielle en cybersécurité :** Cette partie analyse les travaux exploitant des modèles d'apprentissage automatique afin de pallier certaines limites des approches traditionnelles. Elle met en évidence leur utilisation dans la prédiction des vulnérabilités futures, ainsi que les avantages et défis liés à leur mise en œuvre.

## 3.2 ÉTAT DE L'ART SUR L'ANALYSE DES VULNÉRABILITÉS

Les travaux de recherche en cybersécurité s'appuient majoritairement sur la base de données CVE comme référence commune pour l'identification et l'analyse des vulnérabilités. Ces identifiants standardisés sont largement exploités dans la littérature afin d'étudier l'évolution des failles de sécurité, leur répartition temporelle ainsi que les produits affectés

[47]. Cependant, les informations fournies par la CVE restent incomplètes pour comprendre pleinement la vulnérabilité et effectuer une analyse selon plusieurs dimensions. C'est à ce niveau qu'intervient un autre référentiel : la NVD, une base de données publique américaine maintenue par le NIST (National Institute of Standards and Technology) [43]. Elle propose un répertoire enrichi de vulnérabilités de sécurité en s'appuyant sur les enregistrements de la CVE. Contrairement à cette dernière, qui se limite à attribuer un identifiant unique et une description standardisée, la NVD enrichit les données issues de la CVE en ajoutant des métadonnées essentielles, telles que :

1. Scores CVSS : Le score CVSS est largement utilisé dans la littérature comme indicateur synthétique de la sévérité des vulnérabilités. Il permet d'analyser, de comparer et de prioriser les failles de sécurité, et constitue un élément central dans l'évaluation du risque et les processus de gestion et de remédiation. Les travaux existants exploitent principalement les versions v2 et v3 du CVSS pour étudier la distribution de la sévérité des vulnérabilités [43].
2. Types de vulnérabilités (CWE) : Le CWE est une classification normalisée des types de vulnérabilités logicielles et matérielles, mise en place par la MITRE Corporation. Ce référentiel permet de mieux comprendre la nature d'une vulnérabilité en identifiant sa cause profonde et en la rattachant à une catégorie de faiblesse reconnue. La détermination du type de vulnérabilité s'effectue à partir de l'analyse de la description publiée dans le CVE ainsi que des références techniques disponibles, telles que les bulletins de sécurité ou les rapports de chercheurs. Une fois cette correspondance établie, le CWE est intégré directement dans le rapport du NVD comme information pertinente, ce qui facilite la priorisation des correctifs et la prise de décision stratégique en matière de gestion des risques de sécurité [48].

3. Référentiel commun des plateformes (CPE) : Le CPE est un schéma de nommage structuré et standardisé pour les systèmes logiciels et matériels, géré par le NIST. Son objectif est de fournir une méthode uniforme permettant d'identifier de manière unique un produit. Il sert à cibler précisément les produits logiciels ou matériels affectés par une vulnérabilité, ce qui facilite l'automatisation et la gestion des vulnérabilités liées à un produit spécifique. La figure suivante fournit une représentation claire des différents champs composant le CPE [43].

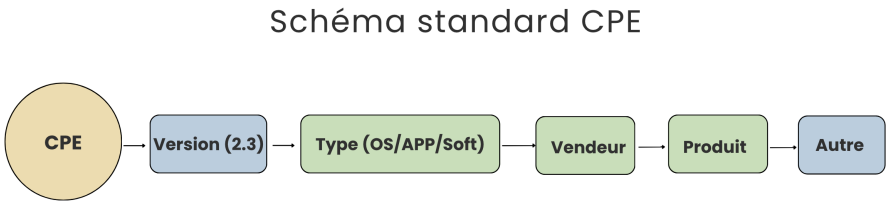


**FIGURE 3.1 : Schéma standard du format CPE v2.3**

La méthode d'accès au site du NIST pour la récupération des données constitue un défi, en particulier lors de l'utilisation de scripts automatisés, en raison des limitations imposées par la plateforme, notamment la restriction du nombre de requêtes par adresse IP sur une période donnée. Cette contrainte empêche la récupération continue des données et rend difficile leur mise à jour en temps réel. Cette problématique peut cependant être résolue par l'utilisation des archives JSON, qui regroupent l'ensemble des vulnérabilités classées par année. L'accès à ces archives est totalement libre et sans restriction, offrant l'avantage de disposer d'un jeu de données complet et à jour [43].

L'exploitation des indicateurs fournis dans les rapports de vulnérabilités permet de générer des statistiques globales, notamment sur la répartition des types d'attaques et sur

les produits présentant le plus grand nombre de vulnérabilités. Cependant, cette exploitation directe reste limitée. En effet, bien que ces données soient accessibles au grand public, elles ne permettent pas de produire des indicateurs personnalisés, nécessaires à une gestion efficace et adaptée des menaces. Une exploitation plus avancée peut toutefois générer des indicateurs plus complexes, améliorant significativement la compréhension du risque [49]. À titre d'exemple, l'évaluation de la fiabilité d'un fournisseur dans la correction des vulnérabilités liées à ses produits, comparée à celle de ses concurrents sur le marché. Cette fiabilité peut être évaluée en analysant le nombre de vulnérabilités critiques affectant ses produits ainsi que le temps de réponse apporté face à chaque menace. Le calcul d'une moyenne de ces mesures peut alors constituer un indicateur de classification des fournisseurs et faciliter la prise de décision des parties prenantes.

### 3.2.1 PRINCIPAUX INDICATEURS EXPLOITÉS DANS LA LITTÉRATURE

Les indicateurs les plus fréquemment abordés dans la littérature sont généralement liés aux informations de base fournies dans les rapports de vulnérabilités. L'analyse de la fréquence des vulnérabilités par année ou par mois constitue l'axe le plus étudié, suivi par l'analyse des vecteurs d'attaque, qui décrivent la manière dont un acteur malveillant peut exploiter une faille. Le score de sévérité demeure également un paramètre important, tout comme le suivi des mises à jour à partir de l'attribut date de modification, permettant d'identifier les changements susceptibles d'affecter une vulnérabilité [21]. Comme précisé précédemment, le CVE fournit pour chaque vulnérabilité une description rédigée en langage naturel, qui constitue un résumé standardisé de la faille. Il contient généralement une explication concise du problème de sécurité identifié, la mention des composants ou produits concernés, ainsi que le type de faiblesse en cause, comme par exemple un dépassement de mémoire tampon ou une injection SQL. La description peut également préciser les conditions dans lesquelles

l'exploitation de la faille est possible et, dans certains cas, les conséquences potentielles sur la confidentialité, l'intégrité ou la disponibilité du système affecté [50].

La description des vulnérabilités est largement utilisée car elle fournit des informations utiles qui aident la prise de décision. Cependant, son exploitation nécessite un important travail de normalisation et de standardisation. En effet, plusieurs limites compliquent son analyse : la variabilité du langage naturel, liée à l'hétérogénéité syntaxique et lexicale ; le manque de normalisation, qui rend difficile l'extraction automatique d'informations ; la longueur variable des descriptions ; ainsi que l'absence fréquente d'informations essentielles [50]. Ces défis montrent que, bien que précieuse, cette source reste complexe à exploiter efficacement.

### 3.2.2 CONTENU PERTINENT DU RÉFÉRENTIEL CVE

Le référentiel CVE met à disposition un ensemble d'informations normalisées permettant l'identification et l'analyse des failles de sécurité [47]. Chaque enregistrement regroupe des attributs relatifs à l'identification de la vulnérabilité, à sa temporalité, à son niveau de sévérité ainsi qu'au contexte de son exploitation. Ces informations constituent la base de nombreuses études exploitant les données publiques du CVE. Elles sont utilisées pour analyser les tendances des vulnérabilités, évaluer la gravité des menaces, prioriser les actions correctives et soutenir la recherche sur la détection et la prédiction des failles [51]. Plusieurs travaux, présentés dans les sections suivantes, s'appuient directement sur ces données pour proposer des approches d'analyse ou d'amélioration des systèmes de gestion des vulnérabilités.

### 3.2.3 VALEUR AJOUTÉE DU RÉFÉRENTIEL NVD

La NVD reprend les informations de base fournies par le CVE et les complète par des métadonnées supplémentaires, renforçant ainsi l'analyse des vulnérabilités. L'apport

le plus significatif réside dans l'intégration du CPE, un système de description normalisé permettant d'identifier précisément les plateformes et produits affectés par une vulnérabilité [43]. Les informations fournies par le CPE facilitent la détection, le suivi et le filtrage des vulnérabilités en fonction d'un environnement technique donné. En enrichissant la description des vulnérabilités, la NVD offre ainsi une base plus complète pour l'analyse, la priorisation des correctifs et la conduite de travaux de recherche en cybersécurité [43].

### 3.2.4 TRAVAUX DE RECHERCHE RÉALISÉS

L'analyse statistique occupe une place importante en cybersécurité, notamment dans la détection des vulnérabilités. Elle permet d'identifier les tendances temporelles, de mesurer la fréquence et la gravité des failles, ainsi que de repérer les produits, fournisseurs ou catégories les plus exposés. Cette approche facilite la hiérarchisation des risques et oriente les actions correctives vers les vulnérabilités critiques [11]. Elle contribue également à vérifier la cohérence des données issues de bases publiques comme le CVE et le NVD, tout en fournissant des indicateurs fiables pour la prise de décision. L'analyse des vulnérabilités liées aux objets connectés constitue un volet essentiel, notamment face à la progression massive de ces dispositifs et à leur sensibilité, en particulier en raison de leurs caractéristiques matérielles souvent limitées, l'évaluation de ces vulnérabilités peut être réalisée selon plusieurs critères, en fonction des données disponibles [5].

La première approche de notre étude repose sur une analyse statistique des vulnérabilités affectant les dispositifs connectés. Cette analyse nécessite l'extraction des appareils IoT à partir d'un large ensemble de produits matériels. Plusieurs études ont cherché à identifier et classifier les produits IoT afin de mieux comprendre les tendances des vulnérabilités et leurs impacts. Cependant, les méthodes existantes d'extraction de dispositifs IoT restent limitées car elles reposent souvent sur des processus manuels, comme ceux présentés par [21], [52],

ou sur l'utilisation de mots-clés [31], [32], ce qui restreint la scalabilité et l'automatisation des analyses. Pour répondre à ces limitations, plusieurs travaux se sont concentrés sur des méthodes d'identification automatique ou semi-automatique des appareils IoT, en s'appuyant sur des approches statistiques ou basées sur les données. Blinowski et Piotrowski [53] ont proposé une méthode de classification des systèmes IoT vulnérables en se basant sur les données CVE et NVD. Leur étude cible les dispositifs matériels physiques opérant dans les couches de perception ou de communication réseau des systèmes IoT et IIoT. Les auteurs ont sélectionné les enregistrements CVE liés au matériel et les ont regroupés manuellement en sept classes distinctes. Un classificateur à vecteurs de support (SVM) a ensuite été entraîné sur ces données afin de prédire la catégorie de nouvelles vulnérabilités, permettant ainsi la reconnaissance automatique des appareils IoT vulnérables. De manière similaire, Sivanathan et al. [54] ont introduit Statistical Fingerprinting, une méthode de classification des appareils IoT dans les environnements intelligents basée sur le trafic réseau. Cette approche exploite des caractéristiques statistiques telles que la fréquence des paquets, la taille des flux et les schémas de communication pour distinguer les appareils IoT des ordinateurs ou des téléphones intelligents, sans dépendre des noms de produits ou de fabricants. Leurs résultats ont démontré une grande précision de classification sur un réseau domestique comprenant divers capteurs, caméras et assistants vocaux. D'autres travaux se sont concentrés sur l'identification à partir de textes et de métadonnées. Feng et al. [55] ont développé ARE, un moteur d'acquisition à base de règles qui extrait et annote automatiquement les informations relatives aux appareils à partir des sites web des fabricants, afin de déterminer leur catégorie, leur fournisseur et leur modèle. Des méthodes comportementales et fondées sur le micrologiciel ont également été explorées. Bezawada et al. [56] ont proposé IoTSense, un modèle d'apprentissage automatique passif entraîné sur les données réseau de divers appareils IoT domestiques, atteignant des taux d'identification compris entre 93 % et 100 %. Oser et al. [57] ont développé SAFER, un cadre semi-automatisé combinant l'analyse du micrologiciel et celle du réseau afin d'extraire des

métadonnées exploitables sur les appareils, incluant le modèle, le fabricant et l'historique des vulnérabilités. Enfin, Siby et al. [58] ont introduit IoTScanner, un cadre de surveillance passive capable de détecter les appareils IoT et les menaces potentielles pour la vie privée dans les environnements sans fil, sans accès direct aux dispositifs.

Ces différentes méthodes d'identification et de classification des appareils IoT vulnérables permettent non seulement de détecter les dispositifs à risque, mais fournissent les données nécessaires pour cartographier ces vulnérabilités au sein de l'architecture globale des systèmes IoT. Dans ce contexte, l'analyse des vulnérabilités peut être organisée selon une approche par couches [59], permettant d'associer chaque menace aux niveaux spécifiques du système et de mieux comprendre l'exposition des dispositifs. D'après [59], la majorité des attaques connues répertoriées par l'organisation internationale Open Web Application Security Project (OWASP) dans son programme OWASP IoT Top 10 ciblent principalement la couche application des objets connectés [60]. Cette couche regroupe les logiciels de base, tels que les systèmes d'exploitation, ainsi que les logiciels de fonctionnement, qui présentent fréquemment des vulnérabilités. Elle constitue ainsi une porte d'entrée privilégiée pour les attaquants, car l'exploitation de ces failles peut compromettre directement la sécurité et la disponibilité des dispositifs IoT [5]. Parmi les menaces les plus répandues, on retrouve en premier lieu les attaques par déni de service distribué (DDoS) et les attaques de l'homme du milieu, qui figurent parmi les plus courantes contre les objets connectés. En troisième position, les attaques par rançongiciel représentent également une menace majeure : elles peuvent cibler aussi bien la couche application que la couche données et services cloud, en particulier lorsque les informations sensibles sont hébergées dans le cloud [30].

Les systèmes d'analyse automatisée proposés par les chercheurs jusqu'à présent ne ciblent pas directement les objets connectés, mais se concentrent sur des aspects spécifiques, comme l'analyse des vulnérabilités liées aux rançongiciel, telle que proposée par Lim et al. [21].

Ces auteurs ont conçu un système d'analyse automatisée des vulnérabilités connues, fondé sur les données CVE Details, NVD et CISA, à l'aide de l'outil Python CVE Analyzer. Leur étude, centrée sur les rançongiciel (2017–2022), met en évidence une augmentation des vulnérabilités exploitées entre 2019 et 2021, avec une prédominance des failles à faible complexité et à fort impact. L'étude repose toutefois sur une analyse de données historiques statiques, sans détection en temps réel ni surveillance dynamique, et se limite aux rançongiciel, en excluant d'autres types de menaces telles que les injections ou les escalades de privilèges. Neuhaus et Zimmermann [61] ont proposé une méthode d'analyse automatique des vulnérabilités basée sur les descriptions textuelles fournies par le CVE et la base NVD. Leur approche repose sur l'allocation de Dirichlet latente (LDA), une technique d'apprentissage automatique non supervisé qui permet d'identifier des ensembles de mots récurrents dans un corpus et de les regrouper en thèmes latents. Plus précisément, LDA cherche à découvrir automatiquement les grandes catégories de vulnérabilités ainsi que les tendances émergentes à partir du texte, sans classification prédéfinie. Dans leur étude, appliquée à près de 39 000 vulnérabilités, la méthodologie comprend le nettoyage et la normalisation des données, l'application de LDA, puis la comparaison des thèmes obtenus avec les catégories CWE afin de valider les résultats. L'approche offre une simplification de l'analyse manuelle et met en évidence des tendances comme la montée des vulnérabilités liées aux serveurs d'applications. Toutefois, elle reste limitée car elle repose uniquement sur les descriptions textuelles des CVE, qui nécessitent souvent un traitement spécifique [10]. Le degré d'automatisation demeure restreint. À partir de cette étude, on constate que les bases de données publiques telles que CVE et NVD n'offrent pas toujours des données entièrement fiables, et que leur utilisation nécessite un traitement préalable avant d'être exploitées dans des travaux de recherche. Dans ce contexte Sabetta et Bezzi [62] en soulignent les limites des bases de données de vulnérabilités telles que la NVD, dont la couverture reste partielle et la qualité inégale, en particulier pour les composants logiciels open source (OSS). Pour pallier ces lacunes, les auteurs proposent une

méthode d'identification automatisée des validations de code correctives à l'aide de techniques d'apprentissage automatique. En traitant les modifications de code comme des documents en langage naturel, leur système combine plusieurs classificateurs afin d'atteindre une précision de 80% et un rappel de 43%. Cette approche, légère et efficace, se démarque par sa simplicité et sa capacité à détecter les correctifs de sécurité sans dépendre des avis officiels, tout en utilisant un volume de données d'apprentissage réduit. La méthode proposé repose sur un jeu de données étiquetées manuellement, issu d'un nombre restreint de projets Java, ce qui peut introduire un biais technologique ou communautaire. De plus, l'approche ne prend pas en compte le facteur temporel ni le degré d'urgence des correctifs [63], et elle ne permet pas une détection en temps réel ni une intégration directe dans des systèmes de surveillance continue.

Parmi les problèmes majeurs liés à la gestion des vulnérabilités, deux limites des bases publiques comme CVE et NVD méritent une attention particulière. D'une part, ces bases n'offrent qu'une couverture partielle des correctifs disponibles car de nombreux correctifs ne sont pas référencés, ce qui complique la remédiation pour les organisations [64]. D'autre part, elles manquent de structuration cohérente, notamment en ce qui concerne les liens explicites entre chaque vulnérabilité et son correctif associé [51]. Cette lacune freine les efforts d'automatisation, nuit à la visibilité globale du risque et retarde les actions correctives, en particulier dans des environnements techniques complexes et hétérogènes. Les correctifs ne sont pas centralisés mais dispersés à travers diverses sources externes (dépôts de code comme GitHub, systèmes de suivi de bugs comme Bugzilla, plateformes communautaires type Stack Overflow) [64]. Cette dispersion et la diversité des formats rendent difficile l'agrégation automatique de l'information dans les outils, ce qui donne aux gestionnaires souvent une vue partielle voire biaisée des correctifs. Face à cette problématique, des chercheurs ont proposé une approche de collecte élargie s'appuyant sur trois sources hétérogènes, à savoir GitHub, Bugzilla et Stack Overflow, afin de centraliser un plus grand nombre de correctifs

[65]. Cette méthode permet de réunir jusqu'à quatre fois plus de correctifs que les approches traditionnelles fondées uniquement sur les bases publiques, renforçant ainsi de manière significative les capacités de détection et de remédiation. Toutefois, certaines limites subsistent, notamment en ce qui concerne la validation automatique de la pertinence des correctifs issus de sources ouvertes, qui demeure une tâche difficile. Par ailleurs, la diversité des formats et l'hétérogénéité des origines génèrent un bruit informationnel non négligeable.

Les techniques d'attaque dans le domaine de la cybersécurité correspondent aux méthodes concrètes qu'un pirate utilise pour exploiter une faille, contourner les protections ou pénétrer illégalement dans un système. Elles décrivent, en quelque sorte, le « mode d'emploi » de l'attaque [66]. Faire le lien entre ces techniques et les failles connues reste un vrai défi. Les bases de données publiques listent bien les vulnérabilités, mais elles n'indiquent presque jamais quelles méthodes les attaquants peuvent utiliser pour les exploiter [11]. Ce manque de connexion directe rend plus difficile la compréhension des scénarios d'attaque concrets, ralentit l'identification des failles réellement exploitables, et complique le travail des analystes pour réagir rapidement face aux menaces. Un travail de recherche a été mené dans ce contexte, visant à développer un outil automatisé basé sur le modèle MPNET, capable de détecter les vulnérabilités logicielles en analysant les descriptions textuelles des techniques d'attaque issues du référentiel MITRE ATT&CK [51], Les chercheurs utilisent un prétraitement partiel et complet des descriptions textuelles d'attaques. Le premier inclut la tokenisation, lemmatisation et suppression des mots vides, tandis que le second nettoie davantage le texte en retirant les citations, URL, caractères spéciaux et espaces superflus.

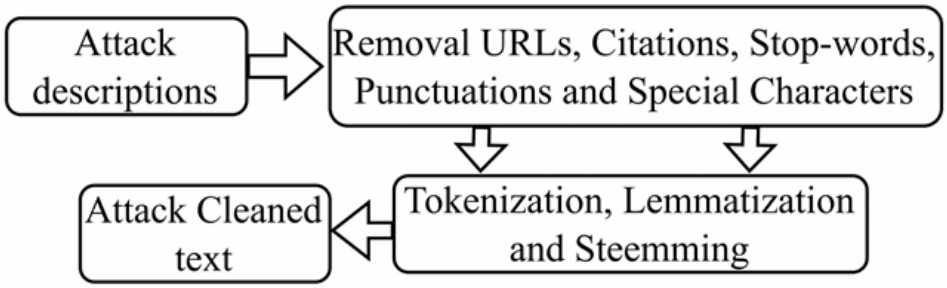


**FIGURE 3.2 : Prétraitement de texte [51]**

L'objectif principal est de combler le fossé entre les descriptions d'attaques et les vulnérabilités référencées dans la base CVE, en facilitant leur mise en correspondance automatique. Pour ce faire, le modèle a été entraîné et évalué sur 100 techniques d'attaque et 685 vulnérabilités, puis comparé à huit autres classificateurs de même catégorie. Les résultats montrent que le modèle proposé offre la meilleure performance surpassant les approches concurrentes. Cependant, l'approche présente certaines limitations. Surtout elle repose uniquement sur les descriptions textuelles des attaques, sans exploiter d'autres métadonnées ou informations contextuelles présentes dans les référentiels MITRE, telles que les vecteurs d'attaque, les tactiques ou les logiciels ciblés [67]. De plus, le modèle a été entraîné sur un jeu de données restreint, ce qui peut limiter sa capacité de généralisation à de nouveaux cas ou à des techniques d'attaque non couvertes par l'ensemble initial [68].

La plupart des outils d'analyse en cybersécurité actuels s'appuient principalement sur des bases de données publiques comme sources pour détecter et corriger les vulnérabilités, mais cette méthode reste largement réactive car elle n'agit qu'après qu'une faille ait été rendue publique, parfois sans correctif disponible. Pour aller plus loin, des chercheurs ont proposé une extension du format CVE [63], appelée Time-Related Vulnerability Lookahead Extension (T-CVE), qui propose d'intégrer à l'analyse des vulnérabilités des informations temporelles susceptibles d'influencer le niveau de risque, même si aucune faille n'a encore été officiellement signalée.

Ce concept vise notamment à prendre en compte :

— la fin de vie ou le support d'une plateforme ou d'un logiciel (OPS),

— l'obsolescence des signatures antivirus ou IPS (OODS),

— la dégradation progressive d'un matériel (SD),

— l'expiration d'une licence, d'un certificat ou d'un service logiciel (ESW).

| CVE | T-CVE |
|---|---|
| Name<br>CVE prefix + Year + Arbitrary Digits | Name<br>T-CVE prefix + Year + Arbitrary Digits |
| Description | Description |
| Status | Status |
| Phase | Phase |
| Reference<br>Multiple sources | Reference<br>There is only one source that should be the reference, vendor source. |
| Vote | (No need) |
| Vote Comment | (No need) |
| (N/A) | Type (Extension)<br>There are 4 types of T-CVE, OPS, OODS, SD, EPS |
| (N/A) | T-CVE Date |

**FIGURE 3.3 : Représentation de l'étude liée au T-CVE [63]**

Cette proposition pourrait considérablement améliorer la prise de décision face aux vulnérabilités encore non détectées. En intégrant des indicateurs temporels, il serait possible de mettre en place une stratégie de gestion proactive, réduisant la fenêtre d'exposition et renforçant la résilience des systèmes. Cependant, malgré son intérêt, le système T-CVE reste pour l'instant un concept théorique car il n'a pas encore été déployé ni validé à grande échelle, et aucun mécanisme complet de calcul du Time-Related Vulnerability Scoring System (TVSS)

ou de conversion automatisée vers des scores qualitatifs n'a été défini. Les auteurs n'ont donc pas pu présenter de résultats expérimentaux, leur étude se limitant à exposer le cadre et la méthodologie envisagés pour une éventuelle mise en œuvre future.

## 3.3 ÉTAT DE L'ART SUR LE DÉLAI DE REMÉDIATION

Comme défini précédemment, le temps de remédiation constitue un paramètre clé pour évaluer la fiabilité d'un fournisseur de produits IoT, en mesurant sa réactivité face aux menaces liées à ses produits. Le calcul de ce paramètre repose sur plusieurs critères et représente un défi en raison du manque de sources fournissant directement les informations nécessaires. Ainsi, certaines recherches ciblent différents aspects afin de faciliter l'obtention des données liées à ce paramètre. Le calcul du temps de remédiation repose principalement sur deux paramètres essentiels : la date de détection d'une vulnérabilité et la date de correction associée. L'obtention de ces deux informations permet de mesurer la durée écoulée entre la découverte et la résolution de la faille. Pour bien appréhender cette mesure, il est nécessaire de comprendre le cycle de vie d'une vulnérabilité, ce qui rejoint directement le cadre d'analyse proposé par Ruohonen et al [69]. L'étude se concentre sur les délais intermédiaires du cycle de vie des vulnérabilités, c'est-à-dire sur la période comprise entre leur détection initiale et leur publication officielle. Plus précisément, elle examine le temps écoulé entre l'attribution d'un identifiant CVE sur la liste publique oss-security et son enregistrement final dans la base National Vulnerability Database (NVD). L'analyse porte sur plus de 5 000 vulnérabilités découvertes entre 2008 et 2016, et s'appuie sur un modèle statistique intégrant environ 50 variables regroupées en trois grandes dimensions :

1. Les réseaux d'interactions entre les acteurs de la sécurité informatique : Cette dimension s'intéresse aux relations professionnelles et techniques entre les individus ou organisations qui participent à la coordination des vulnérabilités. En mobilisant la Social Network Ana-

lysis (SNA), les chercheurs ont cartographié les échanges d'informations au sein de la liste oss-security afin d'identifier les acteurs centraux et la dynamique de collaboration.

2. Les infrastructures de suivi et de gestion des vulnérabilités : Il s'agit des systèmes et plateformes permettant de collecter, documenter et gérer les failles de sécurité telles que la NVD, les bases internes des entreprises ou les systèmes de suivi de bogues (bug tracking systems). Ces infrastructures jouent un rôle clé dans la centralisation des informations et la coordination entre les différents intervenants.

3. Les caractéristiques techniques des vulnérabilités : Cette dimension regroupe les propriétés intrinsèques de chaque faille, comme son type, sa complexité d'exploitation, son score CVSS, ou encore le composant ou système affecté. Ces éléments permettent de mesurer l'impact potentiel et la gravité de chaque vulnérabilité.

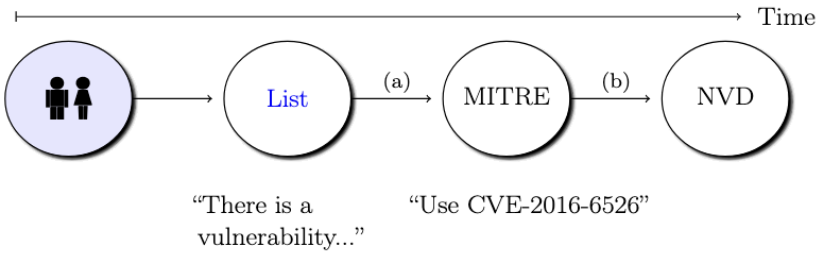


**FIGURE 3.4 : Coordination via oss-security (2008 – 2016) [69]**

Les résultats montrent que les délais sont fortement influencés par des facteurs organisationnels et relationnels, tels que la structure du réseau de coordination, la centralité de certains participants ou encore les contraintes calendaires (effet week-end, variations annuelles). En revanche, l'impact des caractéristiques purement techniques (type de faille, score de gravité) apparaît plus limité. Malgré sa contribution, cette étude demeure statique puisqu'elle repose

sur un intervalle de temps fixe. Or, chaque jour, des milliers de nouvelles vulnérabilités apparaissent dans la base CVE, ce qui rend nécessaire un calcul dynamique et idéalement automatisé du délai de remédiation. Un tel processus suppose plusieurs étapes : l'identification de rapports émis par les fournisseurs, le nettoyage des données issues du web, puis l'extraction d'informations pertinentes lorsque celles-ci existent. Toutefois, la date de détection reste difficile à obtenir, car elle est rarement divulguée par les éditeurs ou les fabricants pour des raisons de sécurité. Ces informations peuvent parfois apparaître dans les rapports finaux de correction ou sur des sites spécialisés. Othmane et al. [70] ont analysé les facteurs influençant le temps nécessaire pour corriger les failles de sécurité dans les logiciels SAP. Pour cela, ils ont comparé trois approches de modélisation : la régression linéaire, le partitionnement récursif et les réseaux de neurones. Les résultats ont montré qu'aucun de ces modèles ne surpassait réellement les autres, et que le type de vulnérabilité (parmi 511 catégories) n'avait pas d'effet significatif sur la durée de correction. Toutefois, cette étude présente plusieurs limites : elle repose uniquement sur des données issues des produits SAP, ne distingue pas clairement les bogues fonctionnels des vulnérabilités de sécurité, et dépend fortement du processus de développement spécifique à SAP, ce qui limite la portée générale des conclusions. Dans la continuité de ces travaux, Yaman et Joseph [71] se sont intéressés à la dynamique temporelle de la publication des correctifs. Ils ont défini le temps de correction comme l'intervalle entre la divulgation d'une vulnérabilité de type zero-day et la publication du correctif correspondant, introduisant un seuil de 120 jours pour distinguer les correctifs « rapides » et « tardifs ». En utilisant l'analyse de survie et la régression de Cox appliquées aux données issues de ZDI et NVD, ils ont montré que plusieurs facteurs influencent la rapidité de correction. Néanmoins, leur étude a également souffert de limitations liées à la qualité et à la cohérence des données disponibles, soulignant la difficulté persistante d'obtenir des ensembles de données exhaustifs et fiables sur les vulnérabilités. En élargissant cette perspective au domaine de l'Internet des objets (IoT), Rudri et al. [72] ont proposé IoTPredictor, un cadre fondé sur les modèles

de Markov cachés pour estimer le temps de correction. En modélisant les transitions des appareils entre des états « sécurisés », « compromis » et « contrefaits », leur méthode calcul la probabilité de restauration d'un dispositif dans une période donnée, soutenant ainsi une gestion proactive des vulnérabilités. De manière similaire, Rivera Álvarez et al. [73] ont exploré la prédiction du temps de correction des vulnérabilités IoT à l'aide de l'analyse de survie combinée au modèle Accelerated Failure Time (AFT) et à XGBoost. En s'appuyant sur des jeux de données publics et privés, ils ont montré que les caractéristiques intrinsèques des vulnérabilités constituent les meilleurs prédicteurs du délai de correction, tandis que les signaux provenant des médias sociaux n'apportent qu'une amélioration marginale. Au-delà du domaine Internet of Things (IoT), Wang et al. [74] ont analysé les pratiques de déploiement des correctifs dans les systèmes de contrôle industriel (ICS). À partir de trois années de données issues de Shodan, couvrant plus de 100 000 dispositifs, ils ont observé qu'environ la moitié étaient corrigés dans un délai de 60 jours, tandis qu'une proportion importante restait vulnérable bien plus longtemps. Pour modéliser ce retard, ils ont adapté le modèle de Bass, obtenant des performances prédictives comparables à celles d'ARIMA, tout en offrant une meilleure interprétabilité.Yang et Abdellatif [75] ont examiné le temps de correction dans l'écosystème Maven, défini comme l'intervalle entre la publication d'un identifiant CVE et la mise à disposition du correctif correspondant. En analysant 3 362 CVE affectant plus de 191 000 versions logicielles, ils ont révélé une forte corrélation entre la sévérité et la rapidité de correction (78 jours pour les vulnérabilités critiques contre 151 pour les faibles) et identifié des caractéristiques propres aux projets telles que le nombre de contributeurs et l'activité des signalements comme facteurs déterminants. L'étude de Rivera et al. (2025) propose une approche prédictive novatrice pour estimer le temps nécessaire à la correction des vulnérabilités IoT, un enjeu crucial face à la prolifération d'appareils souvent commercialisés avec de nombreuses failles de sécurité. Les auteurs s'appuient sur un modèle de type *Accelerated Failure Time* (AFT), implémenté à l'aide de l'algorithme XGBoost, afin de modéliser et de prédire le temps nécessaire à la correction

des vulnérabilités après leur détection. Pour ce faire, ils ont construit une base de données de plus de mille enregistrements en combinant différentes sources, notamment le MITRE, la NVD, VulDB et même Twitter pour capter des signaux sociaux liés aux CVE. Les résultats montrent que les informations issues de la NVD et de VulDB constituent les facteurs les plus déterminants pour accroître la précision des prédictions, tandis que les données sociales ne fournissent qu'une contribution marginale. D'après les chercheurs, cette approche atteint de bonnes performances, puisqu'elle permet d'anticiper les délais de remédiation avec une précision accrue et surpasse à la fois les méthodes purement manuelles et celles entièrement automatiques.cette étude reste limitée par la taille réduite de son échantillon mais elle confirme l'hypothèse selon laquelle la disponibilité des informations sur le Web reste incertaine. Elle met ainsi en évidence l'importance de recourir à des bases publiques structurées et fiables, telles que CVE et NVD, qui constituent des sources indispensables pour renforcer la précision et assurer la reproductibilité des analyses. Une recherche consacrée aux vulnérabilités logicielles [76] propose une méthodologie rigoureuse visant à retracer le cycle de vie complet des failles de sécurité à partir de différentes sources de données. Les auteurs ont constitué un corpus de 735 vulnérabilités liées à l'écosystème Java, publiées entre 2017 et 2022, dont 312 ont été analysées en détail afin d'examiner la chronologie allant de la découverte à la correction puis à la divulgation. Pour ce faire, ils croisent les informations issues des bases publiques (CVE et NVD), des dépôts GitHub et Maven, ainsi que des annonces officielles des fournisseurs et des listes de diffusion. Les résultats révèlent que, dans 77,56 % des cas, les éditeurs publient un correctif avant de divulguer publiquement la vulnérabilité, avec un délai moyen de 16,6 jours entre la mise à disposition du correctif et l'annonce officielle.

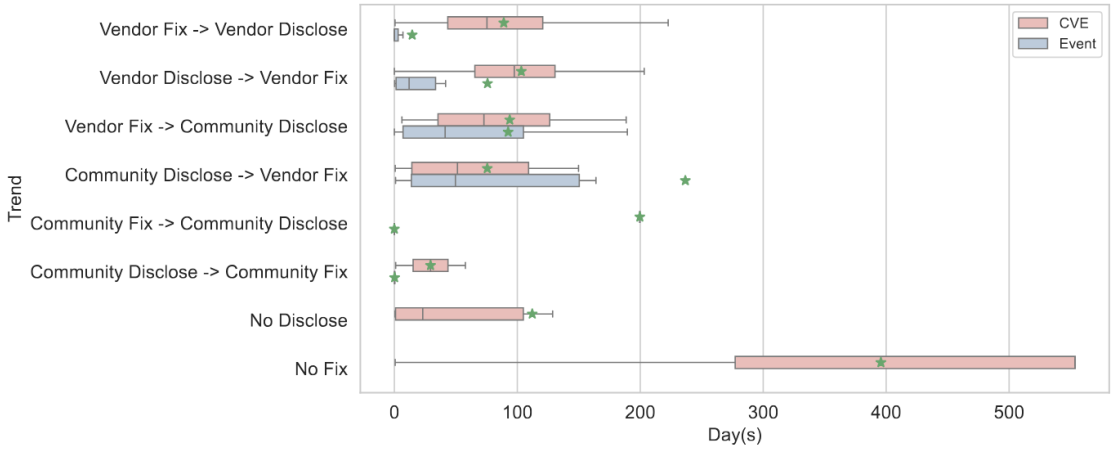


**FIGURE 3.5 : La diversité des scénarios de correction et divulgation [76]**

Cette étude confirme ainsi que la correction d'une vulnérabilité intervient souvent avant sa divulgation publique dans les bases officielles.Comme l'illustre la Figure 3.5 ,elle met également en évidence le rôle crucial des acteurs externes, tels que la communauté scientifique ou des plateformes spécialisées comme la ZDI : lorsqu'une vulnérabilité est signalée par ces contributeurs, les délais de notification et de correction sont significativement réduits. Enfin, les résultats soulignent que les informations relatives aux dates de détection et de correction peuvent être clairement documentées dans certaines plateformes spécialisées, ce qui constitue un apport précieux pour l'analyse du temps de remédiation.

Les travaux abordés dans cette section constituent des pistes de recherche qui traitent, directement ou indirectement, de la problématique du temps de remédiation. Le calcul de ce dernier repose sur deux paramètres essentiels : la date de détection et la date de correction. Selon nos recherches, ces informations sont généralement disponibles dans les rapports de correction publiés par les éditeurs ou dans des plateformes spécialisées reconnues, telles que la ZDI, qui les documentent de manière explicite. Cependant, l'extraction de ces données

demeure complexe, car elle nécessite des processus robustes capables de traiter la diversité des structures rencontrées dans les pages web [77]. Pour rendre ce traitement automatisé plus fiable et reproductible, il est indispensable de s'appuyer sur des sources publiques structurées. Dans ce contexte, les bases comme CVE et NVD apparaissent comme particulièrement intéressantes puisqu'elles offrent des informations pouvant servir de substituts partiels aux dates réelles de détection et de correction [78]. En particulier, la date de réservation fournie par le CVE peut constituer un indicateur proche de la date réelle de détection. Bien qu'elle reste approximative, cette donnée peut s'avérer utile dans les scénarios où un traitement automatisé exige une estimation fiable, notamment lorsqu'aucune autre information explicite n'est disponible. Enfin, il est important de noter que la majorité des études existantes reposent sur des analyses manuelles plutôt que sur des approches automatisées. Ainsi, pour garantir une exploitation pérenne et reproductible, une combinaison d'approches hybrides (incluant des méthodes précises et d'autres approximatives) [79] pourrait représenter une voie prometteuse afin d'assurer la disponibilité et la fiabilité du calcul du temps de remédiation à long terme.

## 3.4 APPLICATION DE L'IA EN CYBERSÉCURITÉ

L'intelligence artificielle constitue aujourd'hui un levier essentiel pour renforcer la cybersécurité. En automatisant la détection, l'analyse et la classification des menaces, les approches d'apprentissage automatique et profond permettent de traiter efficacement de vastes volumes de données provenant de diverses sources d'information sur les vulnérabilités [11]. Cette évolution marque le passage d'une cybersécurité réactive à une approche prédictive, où les modèles d'IA visent à anticiper l'apparition de nouvelles vulnérabilités [80]. Dans ce contexte, la présente revue de littérature se concentre sur les principales contributions à l'application de l'intelligence artificielle pour la prédiction des vulnérabilités futures, en mettant particulièrement l'accent sur l'exploitation des données publiques afin d'anticiper les risques

d'exploitation. Bozorgi et al. [81] ont exploité les données de la NVD (descriptions, dates et références) pour entraîner un modèle supervisé capable de prédire si une vulnérabilité serait exploitée et dans quel délai. Leur étude a montré la valeur prédictive des dépôts publics comme la NVD, non seulement comme sources de documentation, mais aussi comme fondements de décisions. Cependant, la précision du modèle était limitée par la qualité des descriptions textuelles, souvent incomplètes ou inconsistantes. Face à ces limites, Almukainizi et al. [82] ont proposé un modèle hybride combinant données structurées et textuelles pour prédire la probabilité d'exploitation. Les variables catégorielles ont été binarisées, et les descriptions vectorisées avec un modèle Bag-of-Words pondéré par la fréquence des termes. Le jeu de données résultant intègre des attributs de vulnérabilité, des métriques CVSS, des indicateurs linguistiques, ainsi que des mentions provenant du web profond.

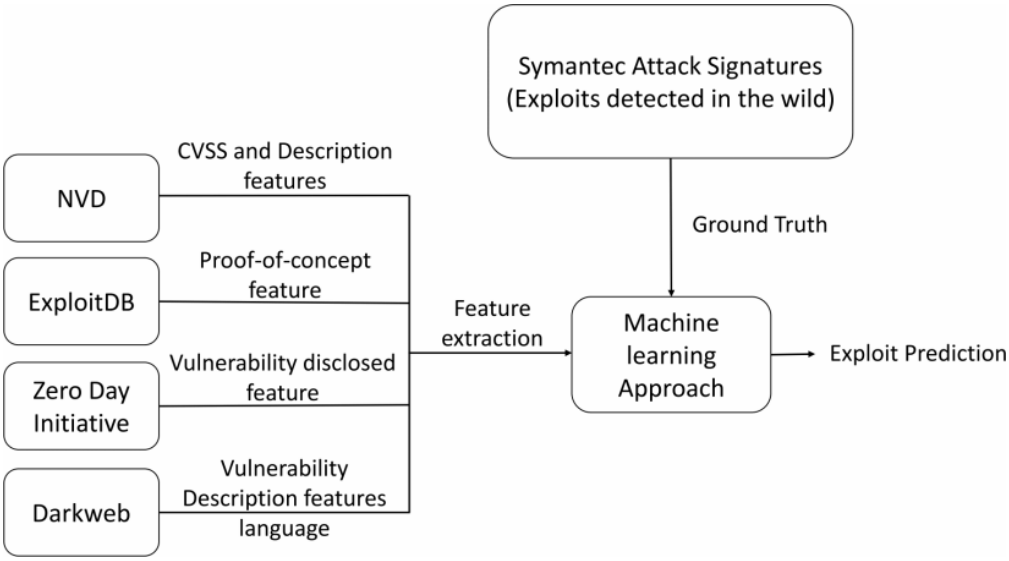


**FIGURE 3.6 : Modèle de prédiction d'exploitation [82]**

L'analyse a utilisé plusieurs classificateurs : Random Forest, SVM, Naive Bayes et régression logistique, Random Forest obtenant le meilleur F1-score. Bien que ce modèle soit efficace pour évaluer l'exploitabilité de vulnérabilités connues, il n'est pas capable d'estimer

quand les exploits pourraient apparaître, et ses résultats restent sensibles à l'intégration des caractéristiques hétérogènes. Cette approche est proche de la nôtre mais demeure réactive, se concentrant sur des vulnérabilités déjà divulguées. D'autres travaux ont cherché à renforcer les modèles prédictifs en intégrant des sources d'information complémentaires, notamment l'activité sur les réseaux sociaux. Sabottke et al. [83] ont ainsi étendu les efforts de prédiction en analysant l'activité sur Twitter pour identifier les vulnérabilités susceptibles d'être exploitées. Ils ont extrait des caractéristiques temporelles, textuelles et d'engagement (volume de tweets, sources, utilisateurs influents), puis entraîné des classificateurs supervisés corrélés avec des bases d'exploits (ExploitDB et jeux de données commerciaux). Les résultats ont démontré que ces signaux provenant des réseaux sociaux amélioraient significativement la priorisation des vulnérabilités par rapport aux heuristiques traditionnelles basées sur le CVSS. Ces approches montrent que l'enrichissement des modèles prédictifs par des signaux externes peut améliorer la priorisation des vulnérabilités à court terme. Pour compléter cette perspective, Kalouptsoglou et al. (2022) [27] proposent d'explorer à la fois des modèles statistiques et des modèles d'apprentissage profond afin de prévoir le nombre de vulnérabilités logicielles dans une fenêtre de 24 mois. Les chercheurs se sont appuyés sur les données de la base NVD et ont ciblé cinq logiciels populaires : Google Chrome, Internet Explorer, macOS, Ubuntu et Microsoft Office. Ils ont construit des séries temporelles mensuelles représentant le nombre de vulnérabilités signalées pour chacun de ces logiciels, puis ont divisé les données en deux ensembles : un jeu d'entraînement et une fenêtre de test de 24 mois. Plusieurs modèles ont été évalués, parmi lesquels des approches statistiques comme le SES, le TES, l'ARIMA et la méthode de Croston, ainsi que des approches d'apprentissage profond incluant le Multi-Layer Perceptron (MLP), les réseaux récurrents classiques (RNN), les LSTM et GRU, le biLSTM et enfin le CNN pour la détection de motifs temporels. Les modèles ont été entraînés sur 24 mois passés afin de prédire les 24 mois suivants et leur performance a été mesurée à l'aide

de la moyenne absolue des erreurs (MAE) et de la racine carrée de la moyenne des erreurs quadratiques (RMSE).

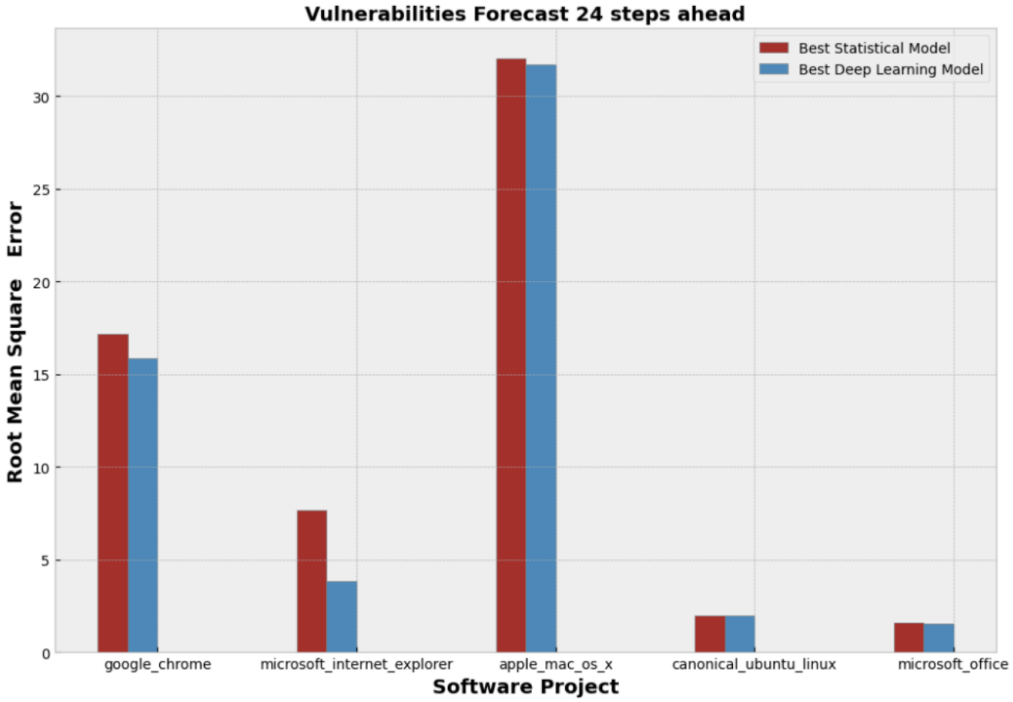


**FIGURE 3.7 : Performance des modèles évaluée par la métrique MAE**

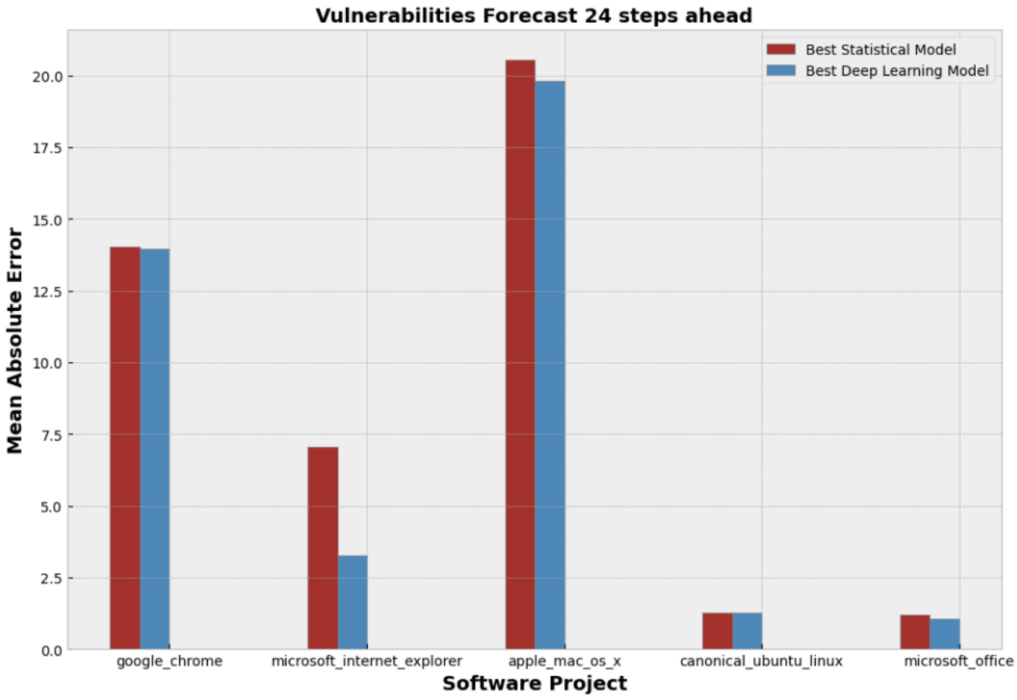


**FIGURE 3.8 : Performance des modèles évaluée par la métrique RMSE**

Les résultats montrent qu'il n'existe pas de modèle universellement performant et que la précision varie selon le logiciel étudié. Globalement, les modèles statistiques fournissent un bon ajustement aux données historiques, tandis que les modèles de deep learning produisent de meilleures prévisions en phase de test, mais avec un gain souvent peu significatif. Une exception notable concerne Internet Explorer, pour lequel les réseaux neuronaux surpassent nettement les méthodes classiques, ce qui conduit les auteurs à conclure que le choix du modèle optimal doit être effectué au cas par cas, en fonction des caractéristiques propres à chaque série de vulnérabilités. Une autre étude menée par Tiwari [28] s'appuie sur les descriptions textuelles des rapports CVE et NVD afin de proposer un modèle de classification automatique basé sur BERT. Contrairement aux approches de prévision par séries temporelles, cette recherche met l'accent sur l'exploitation des descriptions de vulnérabilités pour prédire à la fois leur gravité et leur type. L'architecture repose sur un apprentissage multi-tâches où BERT est

entraîné avec deux sorties parallèles, permettant d'optimiser simultanément la classification de la gravité et celle des types. Les résultats expérimentaux sont particulièrement prometteurs, avec une précision supérieure à 90 % pour les deux dimensions, ce qui démontre l'efficacité de cette approche face aux méthodes classiques de classification. De plus, le système a été déployé sous forme d'API REST et d'une interface Streamlit, ce qui en facilite l'utilisation pratique en temps réel par les analystes de sécurité. Cette étude souligne ainsi le potentiel des modèles de classification basés sur le traitement du langage naturel pour améliorer le triage, la priorisation et la gestion proactive des vulnérabilités, dans un contexte marqué par une croissance continue du volume des CVE. Rivera Álvarez et al. [73] ont développé un modèle combinant analyse de survie et apprentissage automatique afin d'estimer le temps nécessaire à la remédiation des vulnérabilités IoT. En utilisant le modèle Accelerated Failure Time (AFT) et XGBoost, et en s'appuyant sur les données issues de la NVD et de VulDB, ils ont intégré à la fois des caractéristiques classiques (vecteurs CVSS, CWEs, complexité d'exploitation) et des informations textuelles extraites des rapports. Cette approche hybride a permis d'améliorer significativement la précision des prédictions, notamment pour les dispositifs IoT, où le déploiement des correctifs est souvent plus lent et irrégulier. Dans l'ensemble, ces travaux apportent des contributions importantes mais restent majoritairement réactifs, se concentrant sur la prédiction de l'exploitation de vulnérabilités déjà divulguées [81], [84]. De plus, leur dépendance à des données non structurées ou volatiles provenant des réseaux sociaux, forums ou dark web [82], [83] introduit une variabilité qui limite la reproductibilité. À l'inverse, notre approche adopte une perspective proactive, visant à anticiper l'apparition de vulnérabilités encore inconnues à partir de caractéristiques temporelles et quantitatives issues des données CVE/NVD, telles que les séquences de publication, les fréquences et les types de faiblesses (CWEs). Nous comparons plusieurs modèles d'apprentissage automatique pour identifier celui le plus adapté à cette tâche prédictive. Le cadre résultant est entièrement automatisable et scalable, facilitant son intégration dans les pipelines d'analyse de vulnérabilités et représentant

un passage de la détection réactive à la prévention prédictive, mieux adaptée aux dynamiques critiques des systèmes modernes [73].

# CHAPITRE IV
# MÉTHODOLOGIE SCIENTIFIQUE

L'objectif de notre étude est de développer un outil complet intégrant des solutions innovantes, destiné à soutenir la prise de décision dans le domaine de la cybersécurité. Cet outil vise à apporter des réponses à des problématiques identifiées comme critiques dans la littérature, en particulier dans le contexte des objets connectés. Pour atteindre cet objectif, notre recherche s'articule autour de trois axes complémentaires, chacun contribuant à éclairer une dimension spécifique du problème étudié. Premièrement, nous visons à fournir une solution permettant l'extraction et l'analyse des tendances liées aux vulnérabilités affectant les objets connectés. Cette analyse s'appuie sur l'exploitation des bases de données publiques (CVE et NVD), ainsi que sur l'utilisation d'outil d'intelligence artificielle GPT-4o, afin de sélectionner les produits et de structurer les informations disponibles. Deuxièmement, nous proposons une approche innovante pour estimer de façon approximative le temps de remédiation, c'est-à-dire la durée dont un fournisseur a besoin pour corriger une vulnérabilité affectant ses produits. L'analyse de ce délai représente un indicateur clé permettant d'évaluer la réactivité et la fiabilité des fournisseurs face aux menaces de sécurité. Troisièmement, nous avons étudié différents types de modèles d'apprentissage automatique, allant des approches de classification aux modèles de traitement automatique du langage naturel (NLP) et de deep learning, afin d'identifier ceux les plus adaptés à la prédiction de vulnérabilités futures. Ces modèles ont été entraînés et évalués sur un jeu de données temporelles, comprenant à la fois des informations datées et des caractéristiques liées aux vulnérabilités, dans le but de mesurer leur efficacité pour anticiper l'apparition de nouvelles failles sur un horizon défini. Pour garantir l'efficacité de nos approches, il est indispensable de disposer de données complètes et bien structurées.

C'est dans cette optique que nous avons d'abord mis en place un processus rigoureux de collecte et d'agrégation des données, constituant ainsi la base solide de nos analyses.

En résume,cette section présente une description structurée des étapes méthodologiques correspondant aux trois volets de notre étude. Elles incluent la collecte, la préparation, le nettoyage et l'extraction des données, suivies du calcul du temps moyen de remédiation des vulnérabilités et du développement d'une approche dédiée à la prédiction des vulnérabilités futures. L'ensemble repose sur une analyse croisée de trois sources de données reconnues : le répertoire Common Vulnerabilities and Exposures (CVE) maintenu par le MITRE, la National Vulnerability Database (NVD) gérée par le NIST, et la plateforme spécialisée Zero Day Initiative (ZDI). La figure suivante illustre de manière synthétique et structurée les différentes étapes méthodologiques mises en œuvre.

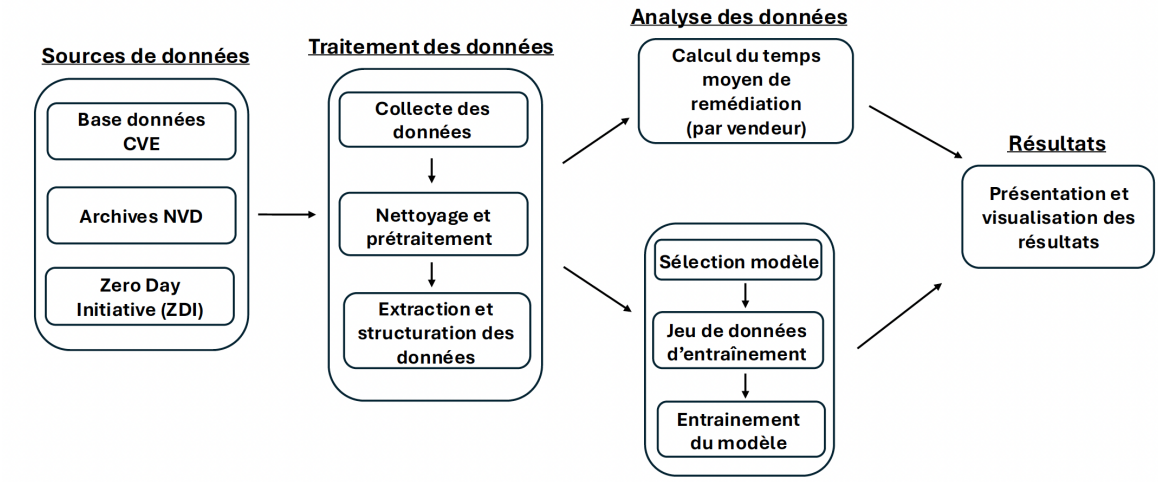


**FIGURE 4.1 : Méthodologie adoptée**

## 4.1 COLLECTE ET AGRÉGATION DES DONNÉES

Les données utilisées dans notre étude proviennent de deux sources principales : le CVE et le NVD. Le CVE constitue la source primaire, car il représente le référentiel central des vulnérabilités connues. Chaque vulnérabilité y est identifiée par un identifiant unique (CVE ID), accompagné d'une description en langage naturel ainsi que de références externes vers des bulletins de sécurité, des rapports techniques ou des annonces officielles [9]. Le *National Vulnerability Database* (NVD) complète ces enregistrements en fournissant une couche d'analyse et de normalisation reposant sur les identifiants CVE. Pour chaque entrée, le NVD enrichit les informations en leur associant plusieurs dimensions d'analyse complémentaires [43] notamment les scores CVSS (Common Vulnerability Scoring System), qui permettent d'évaluer la gravité des vulnérabilités en fonction de critères tels que l'impact ou l'exploitabilité. Il propose également une classification des faiblesses à travers le référentiel CWE (Common Weakness Enumeration), ainsi qu'une identification précise des produits et plateformes affectés grâce au champ CPE (Common Platform Enumeration).

L'agrégation automatique de ces données en temps réel constitue un défi majeur dans le cadre de notre étude. En effet,la collecte peut être effectuée de plusieurs manières, puisque les deux plateformes offrent différents modes d'accès, mais avec certaines restrictions lorsqu'il s'agit de collecter massivement des données.L'accès est possible via les interfaces web officielles, les services API ou encore les archives JSON téléchargeables et classées par année [85]. Dans le cas d'un traitement automatisé, les services API et les archives JSON sont les moyens les plus couramment utilisés. L'utilisation des services API présente cependant certaines limites, notamment la restriction du nombre de requêtes autorisées, ce qui complique l'accès continu aux données dans le cadre d'un système en temps réel.Pour contourner cette contrainte, notre système s'appuie principalement sur les archives JSON, qui constituent une

source plus complète, libre de restrictions majeures, et offrant des informations régulièrement mises à jour.

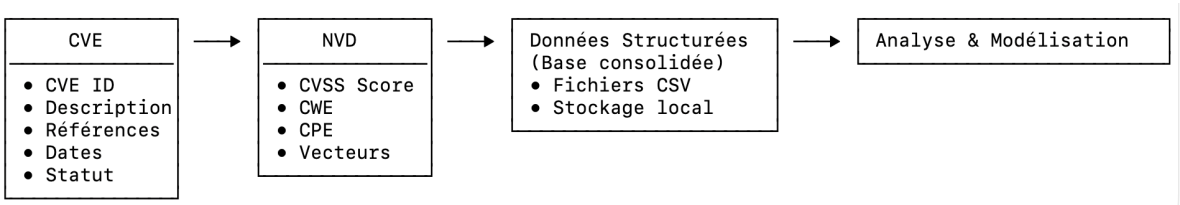


**FIGURE 4.2 : Processus de collecte et d'exploitation des données**

En complément des sources classiques telles que CVE et NVD, la plateforme ZDI a été intégrée à cette étude comme source de vérification. Elle fournit des informations détaillées sur le cycle de traitement des vulnérabilités, incluant à la fois la date de signalement et la date de correction,elle fonctionne selon un modèle de divulgation coordonnée, dans lequel les chercheurs en cybersécurité soumettent leurs découvertes, que la plateforme valide puis transmet aux fournisseurs afin qu'ils puissent les corriger. Une fois la vulnérabilité corrigée, la plateforme rend les informations publiques en incluant ces deux dates, ce qui en fait l'une des rares sources à offrir ce niveau de traçabilité[45]. Dans cette étude, ZDI a été intégrée à la collecte de données comme référence fiable pour l'évaluation du temps réel de remédiation. Les données ont été collectées via l'API et stockées localement dans une base de données structurée, permettant un traitement et une exploitation efficaces dans le cadre de notre analyse.

### 4.1.1 PROBLÉMATIQUE LIÉE À L'EXTRACTION DES IOT

L'identification des objets connectés nécessite un filtrage rigoureux et une sélection spécifique des produits répondant aux critères de l'IoT. L'analyse peut être menée selon plusieurs approches, mais la méthode de traitement des données constitue ici un défi majeur.

En effet, l'extraction des objets connectés à partir des bases publiques de vulnérabilités représente un enjeu complexe. Bien que des bases telles que le CVE et le NVD soient largement exploitées pour l'analyse des vulnérabilités, elles ne fournissent pas d'indications explicites permettant de déterminer si un produit répertorié relève de la catégorie des objets connectés. Cette difficulté est accentuée par la complexité même de la définition de l'IoT, qui désigne un objet connecté comme un dispositif matériel capable d'interagir avec son environnement grâce à des capteurs ou actionneurs, doté d'une capacité de traitement locale, capable d'échanger des données via réseau filaire ou sans file, et fonctionnant de manière autonome sans intervention humaine directe [38].

Aujourd'hui, plusieurs études proposent des analyses statistiques portant sur les objets connectés en s'appuyant sur les rapports publics tels que le CVE et le NVD. Toutefois, un élément déterminant réside dans la précision du ciblage des objets connectés, car une mauvaise identification peut fausser les résultats.Dans la littérature,les méthodes d'extraction proposé commencent par l'identification des produits matériels à partir du champ CPE,puis chaque étude adopte ensuite ses propres paramètres de sélection : certaines exploitent des mots-clés pour cibler des catégories spécifiques (par exemple, les caméras de surveillance) [86], tandis que d'autres croisent les données issues du CVE/NVD avec des sources externes, comme Shodan, afin de confirmer qu'un produit appartient bien à l'IoT [87]. Toutefois, cette dernière approche peut s'avérer coûteuse dans un traitement automatisé. Par ailleurs, certains travaux recourent à des modèles de traitement automatique du lanµgage (NLP) comme BERT afin d'analyser les descriptions textuelles des vulnérabilités[88] ,la précision de ces modèles reste fortement dépendante de la qualité et de l'étendue des jeux de données d'entraînement, ce qui limite leur efficacité. Cela souligne la nécessité de développer des approches plus robustes et précises pour améliorer le ciblage des objets connectés dans ce type d'analyse.

### 4.1.2 APPROCHE PROPOSÉE POUR L'EXTRACTION DES IOT

Notre approche repose sur l'hypothèse suivante : la fiche technique constitue la source la plus fiable pour déterminer si un produit matériel appartient à la catégorie des objets connectés. L'accès automatisé à ces fiches techniques nécessite un modèle d'IA en ligne, capable de les consulter en temps réel. Ces documents étant généralement accessibles au public et aux consommateurs, une simple navigation peut suffire pour leur récupération et leur analyse.Parmi les modèles d'intelligence artificielle en ligne disponibles, Shahriar et al. [89] ont mené une évaluation comparative des performances. Leur étude expérimentale propose une analyse approfondie des capacités linguistiques, visuelles, vocales et multimodales. Les résultats montrent que GPT-4o surpasse ses prédécesseurs, grâce à ses performances renforcées en traitement du langage, en raisonnement, en classification d'images et en reconnaissance vocale.

| Category/Model | Deductive Reasoning | | Inductive Reasoning | | Abductive Reasoning |
|---|---|---|---|---|---|
| | Entailment Bank | bAbI (Task 15) | CLUTRR | bAbI (Task 15) | $\alpha$NLI |
| GPT-3.5 | 25/30 | 26/30 | 2/30 | 14/30 | 19/30 |
| GPT-4 | 27/30 | 30/30 | 11/30 | 28/30 | 25/30 |
| GPT-4o | 29/30 | 30/30 | 17/30 | 30/30 | 27/30 |

**FIGURE 4.3 : Performance des modèles GPT dans les tâches de raisonnement logique** [89]

Les premières versions de GPT ne disposaient pas d'un accès direct et en temps réel à Internet, ce qui limitait leur capacité à exploiter des données actualisées. Avec l'introduction de GPT-4o, des améliorations notables ont été apportées, notamment l'intégration d'un mode « browsing ». Ce mode permet au modèle de consulter en direct des pages web, des fiches techniques ou des bases de données publiques afin d'accéder à des informations récentes et vérifiables. L'interrogation du modèle s'effectue au moyen de requêtes structurées, ce qui

garantit un processus d'analyse reproductible et une évaluation plus fiable des résultats.une requête bien structurée conçue pour exploiter le modèle ChatGPT-4o afin de déterminer si un produit donné correspond à la définition stricte d'un objet connecté (IoT). Le rôle du système définit le contexte : le modèle est chargé d'agir en tant qu'expert en cybersécurité et doit appliquer des critères précis, à savoir qu'un IoT est un objet physique connecté à Internet, capable de collecter, transmettre et traiter des données sans intervention humaine directe. La partie contenu utilisateur fournit les informations sur le ou les produits à analyser, incluant le nom, le fournisseur et éventuellement le modèle, la série ou le SKU. Pour améliorer la précision, la requête inclut également des preuves documentaires via les champs `evidence_urls` et `evidence_snippets`, permettant au modèle de consulter les fiches techniques, manuels et pages produit afin d'identifier la connectivité, la collecte de données et les fonctionnalités autonomes. Les vérifications imposent les critères stricts à respecter pour valider qu'un produit est IoT, et le champ output spécifie que la réponse doit être fournie au format JSON structuré, incluant pour chaque produit la décision IoT (oui/non), le niveau de confiance et la justification fondée sur les preuves. Cette structure garantit que la requête est à la fois rigoureuse, répétable et exploitable pour l'évaluation académique ou automatisée d'un ensemble de produits.

```
{
  "role": "user",
  "content": {
    "request_id": "UUID",
    "timestamp_utc": "YYYY-MM-DDTHH:MM:SSZ",
    "source": "user | csv | crawler",
    "product": {
      "name": "Nom du produit",
      "vendor": "Nom du fournisseur",
      "model": "Modèle (optionnel)",
      "series": "Série (optionnel)",
      "release_year": "2023",
      "category": "smart_home",
      "connectivity": ["Wi-Fi", "Bluetooth"],
      "sensors": ["temperature", "humidity"],
      "autonomous_functions": ["temperature control", "remote alerts"]
    },
    "evidence_urls": ["Lien vers fiche produit, manuel ou datasheet"],
    "evidence_snippets": ["Extraits textuels décrivant connectivité, collecte de données et action
    autonome"],
    "checks": {
      "require_physical_device": true,
      "require_connectivity": true,
      "require_data_collection": true,
      "require_data_transmission": true
    },
    "output": {
      "format": "json",
      "include_rationale": true,
      "include_sources": true
    }
  }
```

**FIGURE 4.4 : Structure de la requête utilisée avec le modèle GPT-4o**

Afin d'assurer la fiabilité du processus, une évaluation systématique des réponses générées par le modèle a été réalisée pour chaque version du prompt. Cette évaluation s'est appuyée sur la méthode *GPTScore*, reconnue comme l'un des outils les plus efficaces pour l'évaluation automatique de textes générés par l'IA [90]. Le modèle a ainsi agi en tant que juge automatisé (*LLM-as-a-Judge*), recevant le prompt, la réponse générée et une grille d'évaluation prédéfinie couvrant cinq critères : pertinence, exactitude factuelle, clarté, exhaustivité et qualité globale. Chaque dimension a été notée et accompagnée d'une brève justification.Les scores obtenus ont permis d'évaluer l'évolution de la qualité des réponses entre les différentes

versions du prompt. Cette analyse automatisée a été complétée par une vérification manuelle sur un échantillon de produits afin de renforcer la fiabilité de l'évaluation. Le tableau suivant présente la comparaison des résultats obtenus selon les différentes versions du prompt.

**TABLEAU 4.1 : Évolution de la qualité des réponses en fonction des versions du prompt (Évaluation GPTScore)**

| Version | Pertinence | Exactitude | Clarté | Exhaustivité | Qualité globale | Moyenne (/5) |
|---|---|---|---|---|---|---|
| Version 1 | 1 | 1 | 2 | 1 | 1 | 1.2 |
| Version 2 | 3 | 2 | 3 | 1 | 2 | 2.2 |
| Version 3 | 4 | 4 | 3 | 2 | 3 | 3.2 |
| Version 4 | 5 | 5 | 4 | 4 | 4.5 | 4.5 |
| Version 5 | 5 | 5 | 5 | 5 | 5 | 5.0 |

Le choix de GPT-4o pour l'identification des dispositifs IoT se justifie par sa capacité à générer des réponses précises et fiables. Nous avons mené une étude comparative avec des travaux existants utilisant le même jeu de données IoT_Sentinel [91], afin d'évaluer les performances dans des conditions identiques. Les réponses générées par GPT-4O ont été publiées et mises à disposition sur GitHub [92], garantissant la transparence et la reproductibilité de l'étude.

**TABLEAU 4.2 : Comparaison des performances des méthodes d'identification des dispositifs IoT**

| Étude | Précision (%) | Rappel (%) | F1-Score (%) |
|---|---|---|---|
| Opoku et al., 2025 [66] | 94,20 | 92,50 | 95,00 |
| Hussain et al., 2025 [62] | 91,00 | 91,00 | 91,00 |
| Résultats GPT-4O | 100,00 | 96,77 | 98,37 |

Les résultats présentés dans le tableau 4.2 confirment que GPT-4O dépasse significativement les méthodes existantes en termes de précision, rappel et F1-score. Cette supériorité démontre l'efficacité du modèle pour identifier les dispositifs IoT à partir des spécifications techniques et des données de trafic réseau. Elle souligne également la pertinence de l'approche

proposée, qui combine l'accès en temps réel aux fiches techniques et l'exploitation d'un modèle d'IA avancé. Ces performances élevées garantissent non seulement une meilleure exactitude dans la classification des objets connectés, mais assurent également une reproductibilité et une fiabilité accrues des analyses, constituant un atout majeur pour les études et applications en cybersécurité.

## 4.2 TEMPS DE REMÉDIATION DES VULNÉRABILITÉS

Cette section présente la méthodologie adoptée pour estimer le temps de remédiation des vulnérabilités. Le calcul de ce délai constitue une étape essentielle pour évaluer la réactivité des fournisseurs face aux vulnérabilités signalées. Pour ce faire, il est nécessaire d'identifier deux dates clés qui encadrent le processus de correction : date de découverte correspondant au moment où la vulnérabilité est portée à la connaissance du fournisseur, et date de publication du correctif correspondant au moment où une solution est rendue accessible au public.Notre méthodologie repose sur une approche hiérarchique rigoureuse, conçue pour extraire ces deux dates à partir de sources public fiables, ce qui permet de calculer le délai de remédiation de manière cohérente et reproductible.

### 4.2.1 APPROCHE D'OBTENTION DE LA DATE DE DÉCOUVERTE

Pour estimer la date de découverte ou de signalement des vulnérabilités, nous commençons par analyser les bulletins de sécurité publiés par les fournisseurs. À cette fin, un script Python est utilisé pour extraire automatiquement les informations pertinentes et analyser le contenu de ces bulletins, en se basant sur les liens préalablement enregistrés dans une base de données. Certains bulletins mentionnent explicitement la date de découverte à l'aide d'expressions telles que « Reported on… » ou « Discovered on… » [93]. Cette méthode est plus fiable pour les grands fournisseurs, tels que Google ou Microsoft, qui publient régulièrement des

bulletins de sécurité détaillant les correctifs appliqués. Cependant, elle présente des limites pour les fournisseurs moins connus, souvent nombreux dans l'écosystème IoT, qui fournissent rarement des informations complètes ou structurées sur leurs correctifs. Pour pallier cette limitation, nous adoptons une approche complémentaire et pragmatique basée sur l'hypothèse formulée et soutenue par Ruohonen (2023) [94], selon laquelle la date de réservation d'une vulnérabilité dans les entrées NVD est généralement proche de sa date réelle de divulgation publique. Cette hypothèse nous permet d'estimer la date de signalement initiale avec une précision raisonnable, même en l'absence d'informations explicites.

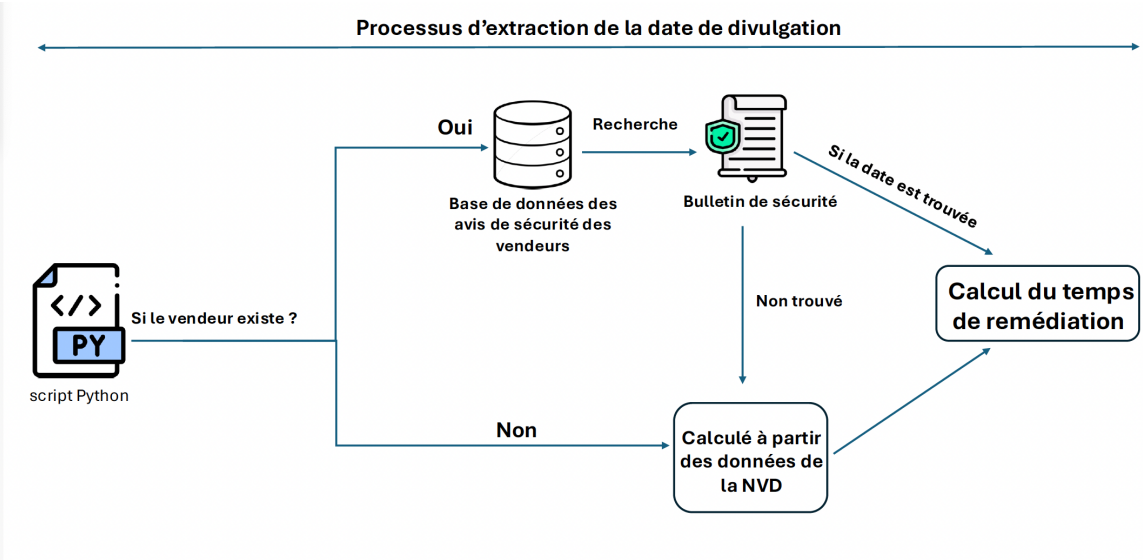


**FIGURE 4.5 : Processus d'extraction de la date de découverte**

Pour valider empiriquement cette hypothèse, nous avons mené une analyse sur un échantillon de 100 enregistrements CVE, en comparant leurs dates de réservation (*dateReserved*) avec leurs dates officielles de divulgation, collectées directement depuis la base ZDI. Les résultats montrent que la date de réservation suit la date de découverte initiale avec une moyenne d'environ 34 jours et une médiane de 27 jours, confirmant que les deux événements

sont généralement séparés par un délai relativement court. Cette proximité temporelle justifie l'utilisation du champ *dateReserved* comme indicateur fiable de la date de découverte ou de signalement lorsqu'aucune information explicite n'est disponible.

**TABLEAU 4.3 : Écarts temporels entre les données CVE et la date effective de découverte.**

| Champ CVE | Différence moyenne (jours) | Différence médiane (jours) |
|---|---|---|
| `dateReserved` | 34 | 27 |
| `publishedDate` | 171 | 82 |
| `lastModifiedDate` | 205 | 135 |

Dans les cas où la date réelle de découverte ou de signalement est indisponible, nous l'estimons à partir du décalage temporel médian [95] observé entre les dates de découverte et de réservation dans notre jeu de données empirique. Plus précisément, la date de découverte peut être approximée comme suit :

$$t^*_{\text{discovery}} = \begin{cases} t_{\text{reserved}} - \delta_{\text{median}}, & \text{si } t_{\text{reserved}} - \delta_{\text{median}} \geq 1 \\ 1, & \text{si } t_{\text{reserved}} - \delta_{\text{median}} < 1 \end{cases}$$

$$\delta_{\text{median}} = 27 \text{ jours.}$$

où :

— $t^*_{\text{discovery}}$ désigne la date de découverte estimée,

— $t_{\text{reserved}}$ correspond à la date de réservation de la CVE (champ *dateReserved*),

— $\delta_{\text{median}}$ représente le délai médian observé entre la date réelle de découverte (source ZDI) et la date de réservation.

Cette formule permet de maintenir une cohérence temporelle dans l'analyse des vulnérabilités, tout en évitant les valeurs négatives ou non plausibles, comme observé dans certains

cas, car le choix de la médiane reste une approximation dépendant de l'échantillon de données disponible. Ainsi, toute modification de ce jeu de données peut influencer les calculs et les estimations obtenues.

### 4.2.2 MÉTHODE D'OBTENTION DE LA DATE DE CORRECTION

À ce jour, aucune source ne permet d'identifier de manière précise et uniforme la date exacte de correction d'une vulnérabilité. Toutefois, le processus officiel de remédiation se conclut par la publication d'un rapport dans la base NVD, décrivant la vulnérabilité et associé à une date de publication. D'après notre revue de la littérature, cette dernière constitue le seul repère temporel fiable et standardisé permettant d'estimer la date effective de correction.

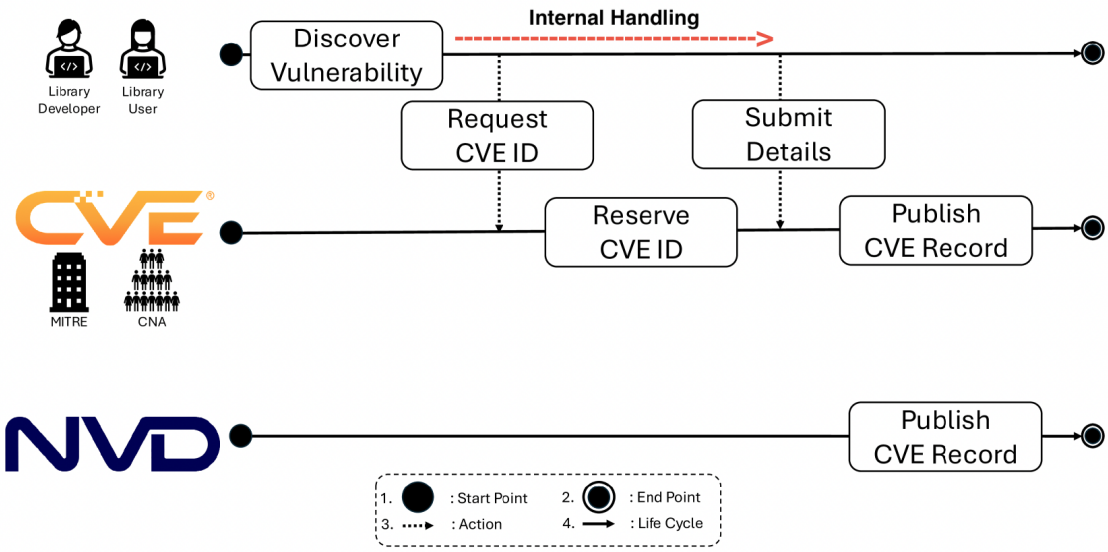


**FIGURE 4.6 : Cycle de vie des vulnérabilités**

Dans le cadre de cette étude, la date de publication du correctif indiquée dans la base NVD est ainsi considérée comme la date officielle de correction de la vulnérabilité. Ce choix

repose sur des justifications méthodologiques et empiriques issues de travaux antérieurs, ainsi que sur des recommandations institutionnelles.Plusieurs études ont adopté la même approche afin de garantir la comparabilité et la reproductibilité des résultats entre fournisseurs. Arora et al. [96] mesurent la réactivité des fournisseurs à partir des dates de publication officielles des correctifs, qu'ils considèrent comme les seules informations observables et vérifiables à grande échelle. Cette date correspond au moment où le correctif devient accessible aux utilisateurs, marquant ainsi le début de la phase de remédiation. De même, Li et Paxson [97] analysent plus de 10 000 correctifs de sécurité publiés par divers fournisseurs et adoptent la même méthode. Ils expliquent que la date de publication est le seul point temporel cohérent et standardisé permettant une comparaison inter-fournisseurs des pratiques de correction, les dates internes de développement n'étant ni publiques ni harmonisées.Dans la même optique, Ruohonen et Hyrynsalmi [98] s'appuient sur les dates de publication pour étudier la coordination entre les CVE Numbering Authorities (CNAs), soulignant que les correctifs non publiés ne disposent pas d'un horodatage uniforme.Enfin, la recommandation NIST SP 800-216 [95], alignée avec la norme ISO/IEC 29147, stipule que les rapports de vulnérabilités doivent indiquer la date à laquelle la correction devient publiquement disponible, ce qui marque la fin du processus de remédiation. Par conséquent, la date de publication fournie dans les rapports du NVD demeure reste l'indicateur le plus fiable de la date réelle de correction. Bien qu'elle puisse légèrement différer de la date d'achèvement interne du développement du correctif, elle reste le seul repère temporel standardisé, vérifiable et reproductible à grande échelle. Ce choix garantit la transparence, la cohérence et la comparabilité des analyses menées dans cette étude.

### 4.2.3 CALCUL DU TEMPS DE REMÉDIATION

Une fois les dates de découverte et de publication du correctif déterminées, le temps de remédiation pour chaque vulnérabilité $v$ est calculé comme suit :

$$T_{\text{remediation}}(v) = t_{\text{fix}}(v) - t^{*}_{\text{discovery}}(v)$$

où :

— $t_{\text{fix}}(v)$ est la date de publication du correctif (ex. *publishedDate*) ;

— $t^{*}_{\text{discovery}}(v)$ est la date de découverte estimée

Pour chaque fournisseur $f$, le temps de remédiation moyen est ensuite obtenu par :

$$\overline{T}_{\text{remediation}}(f) = \frac{1}{|V_f|} \sum_{v \in V_f} T_{\text{remediation}}(v)$$

Cette métrique fournit une mesure cohérente et comparable de la réactivité des fournisseurs face aux vulnérabilités signalées.

## 4.3 PRÉDICTION DES VULNÉRABILITÉS FUTURES

La prédiction des vulnérabilités futures dans les dispositifs IoT repose sur l'analyse temporelle des vulnérabilités publiées historiquement. Cependant, les dates de publication présentent une distribution fortement irrégulière, ce qui complique l'entraînement des modèles d'intelligence artificielle et limite leur capacité à détecter des motifs temporels cohérents. Pour surmonter cette limitation, nous avons mis en œuvre une méthode de reconstruction temporelle permettant de créer un jeu de données régulier et équilibré, adapté à l'apprentissage prédictif. Cette approche s'inspire de travaux récents sur la modélisation des séries temporelles

irrégulières, qui soulignent l'importance de transformer les séquences discontinues ou non uniformes en intervalles réguliers pour les tâches d'apprentissage [99].

### 4.3.1 STRUCTURATION DES DONNÉES

Toutes les vulnérabilités liées à l'Internet des objets (IoT) publiées entre 2019 et 2024 ont été extraites de la *National Vulnerability Database* (NVD). Le choix de cette période est motivé par la croissance exponentielle des dispositifs IoT au cours de ces années, accompagnée d'une augmentation significative du nombre de vulnérabilités publiées [100]. Pour chaque enregistrement, le nom du produit et la date officielle de publication (*publishedDate*) ont été conservés, formant ainsi une série temporelle spécifique à chaque produit IoT.

### 4.3.2 INTERVALLE MOYEN ENTRE VULNÉRABILITÉS

Pour chaque produit $p$, l'intervalle moyen entre deux vulnérabilités successives a été calculé selon la formule suivante :

$$\bar{\Delta}_p = \frac{1}{n-1} \sum_{i=1}^{n-1} (t_{i+1} - t_i) \tag{4.1}$$

où :

— $t_i$ désigne la date de publication de la $i^{\text{e}}$ vulnérabilité,

— $n$ est le nombre total de vulnérabilités pour le produit $p$,

— $\bar{\Delta}_p$ est exprimé en jours.

Les valeurs obtenues pour chaque produit ont été utilisées pour évaluer la distribution des intervalles moyens au sein du corpus IoT. Pour définir une granularité temporelle uniforme, nous avons retenu [101] :

$$\Delta = \max(\bar{\Delta}_p) \tag{4.2}$$

c'est-à-dire la valeur maximale des intervalles moyens observés parmi les produits IoT. Ce choix assure une couverture temporelle complète et une cohérence globale du jeu de données, tout en évitant un biais en faveur des produits avec des fréquences de signalement de vulnérabilités plus élevées. Dans notre étude, cette valeur a été fixée à $\Delta = 7$ jours, correspondant à la période moyenne maximale observée entre deux vulnérabilités publiées.

### 4.3.3 GÉNÉRATION D'UNE SÉRIE TEMPORELLE RÉGULIÈRE

La période d'observation (2019–2024) a été divisée en intervalles réguliers de $\Delta = 7$ jours. Pour chaque produit et chaque instant $t$, une étiquette binaire a été attribuée indiquant si une nouvelle vulnérabilité a été publiée dans les sept jours suivants.Pour chaque instant temporel, une annotation a été effectuée comme suit :

— **1 (positif) :** si au moins une vulnérabilité a été publiée dans les sept jours suivants ;

— **0 (négatif) :** sinon.

### 4.3.4 GESTION DU DÉSÉQUILIBRE

Malgré la régularisation temporelle appliquée, le jeu de données reste déséquilibré, avec environ 67% d'observations négatives contre 33% d'observations positives. Pour remédier à ce déséquilibre sans altérer la structure temporelle du jeu de données, une deuxième approche a été mise en œuvre : la *pondération des classes*. Cette méthode, largement utilisée dans les études de prédiction de vulnérabilités [102], [103], ajuste la fonction de perte de l'algorithme d'apprentissage en attribuant un poids plus élevé aux instances de la classe minoritaire. Les poids de classe sont calculés selon la formule suivante [104] :

$$w_i = \frac{N}{C \times n_i}$$

où :

— $N$ représente le nombre total d'échantillons sur la période d'observation (intervalles temporels générés pour les produits IoT) ;

— $C$ est le nombre total de classes, ici deux : 0 (négatif) et 1 (positif) ;

— $n_i$ indique le nombre d'échantillons appartenant à la classe $i$.

Ainsi, les classes minoritaires reçoivent un poids plus élevé, ce qui augmente leur influence lors de l'entraînement du modèle tout en préservant la cohérence temporelle des données. Cet ajustement équilibre efficacement la contribution des deux classes lors de l'apprentissage et améliore la capacité du modèle à détecter les occurrences rares de vulnérabilités sans modifier la distribution initiale des données. Plusieurs types de modèles prédictifs ont été entraînés sur ce jeu de données afin d'évaluer la configuration offrant les meilleures performances en termes de précision, rappel et score F1 [105].

## 4.4 CONCLUSION

Dans ce chapitre, nous avons présenté la méthodologie générale de notre étude, articulée autour de trois étapes principales : la collecte des données, l'estimation du temps de remédiation et la prédiction des vulnérabilités futures. La première étape de notre travail consisté à construire un ensemble de données complet et cohérent à partir des bases publiques NVD et CVE. Dans ce contexte, nous avons abordé la problématique liée à la sélection des dispositifs IoT et proposé une approche méthodologique visant à assurer une sélection efficace, fiable et représentative, garantissant ainsi la pertinence du jeu de données pour les analyses ultérieures. La deuxième étape a introduit une méthode d'estimation du temps de remédiation fondée sur

la corrélation entre les dates de divulgation et de publication, offrant une mesure objective de la réactivité des fournisseurs face aux vulnérabilités signalées. Enfin, la troisième étape a porté sur la prédiction des vulnérabilités futures. En s'appuyant sur une reconstruction temporelle des données et sur des modèles d'apprentissage supervisé, cette approche vise à anticiper l'apparition de nouvelles failles à court terme dans les produits IoT. Cette méthodologie fournit un cadre rigoureux pour comprendre et modéliser le comportement temporel des vulnérabilités. Elle ouvre la voie à une analyse prédictive plus fine du risque, capable de soutenir la détection proactive et la gestion anticipée des menaces dans l'écosystème IoT. Le chapitre suivant présentera les résultats expérimentaux obtenus à partir de cette méthodologie et évaluera la performance des différents modèles prédictifs proposés.

# CHAPITRE V
# RÉSULTATS

Dans ce chapitre, nous présentons les résultats de notre étude empirique, obtenus grâce à l'application de la méthodologie proposée pour répondre aux questions de recherche définies.

Nous commençons par la présentation des résultats issus de l'analyse des vulnérabilités IoT recensées dans les bases de données CVE et NVD entre 2019 et 2024, selon la méthode de collecte proposée. Ces résultats portent sur les tendances annuelles, les vecteurs d'attaque, les niveaux de gravité, les types d'attaques les plus fréquents et les catégories de dispositifs les plus exposées. Ils incluent également l'évaluation des profils de sécurité des principaux fournisseurs et des produits IoT critiques, afin de mettre en évidence les écarts entre le nombre de vulnérabilités signalées et leur criticité.

La section suivante se concentre sur l'estimation du temps de remédiation des vulnérabilités pour différents fournisseurs. Les résultats obtenus avec notre approche méthodologique sont comparés à ceux de la Zero Day Initiative (ZDI), permettant d'évaluer la précision de notre méthode et de mieux comprendre la précision de l'approche en face des résultat exacte et évaluer la réactivité de quelques fournisseurs selon les diponibles face aux vulnérabilités.

Enfin, nous examinons la capacité prédictive des modèles d'apprentissage automatique et profond pour anticiper l'apparition de nouvelles vulnérabilités dans les dispositifs IoT. Plusieurs algorithmes, tels que Random Forest, XGBoost, LSTM et BERT, sont comparés afin d'identifier le modèle le plus performant pour la prédiction à court terme des vulnérabilités. Cette analyse met en évidence le potentiel des approches prédictives pour soutenir une cybersécurité proactive dans l'écosystème IoT.

L'objectif est de fournir une vision globale des tendances de vulnérabilités, de la performance des fournisseurs en matière de remédiation et de l'efficacité des modèles prédictifs.

## 5.1 ANALYSE DES TENDANCES DANS L'ÉCOSYSTÈME IOT (RQ1)

Cette section présente les tendances observées sur les dispositifs IoT entre 2019 et 2024, à partir des données extraites selon notre approche méthodologique.

### 5.1.1 ÉVOLUTION ANNUELLE DES VECTEURS D'ATTAQUE

Les vecteurs d'attaque correspondent au type d'accès nécessaire pour exploiter une vulnérabilité. Chaque enregistrement CVE contient cette information, permettant d'évaluer comment une vulnérabilité peut être exploitée, que ce soit à distance, localement, physiquement ou via des réseaux adjacents. La méthodologie adoptée permet de collecter l'ensemble des vulnérabilités IoT sur la période étudiée. Pour chaque vulnérabilité, nous avons ciblé la section relative au vecteur d'attaque afin d'identifier ceux associés aux dispositifs IoT et de déterminer les méthodes les plus fréquemment exploitées. Les résultats sont présentés dans la figure 5.1.

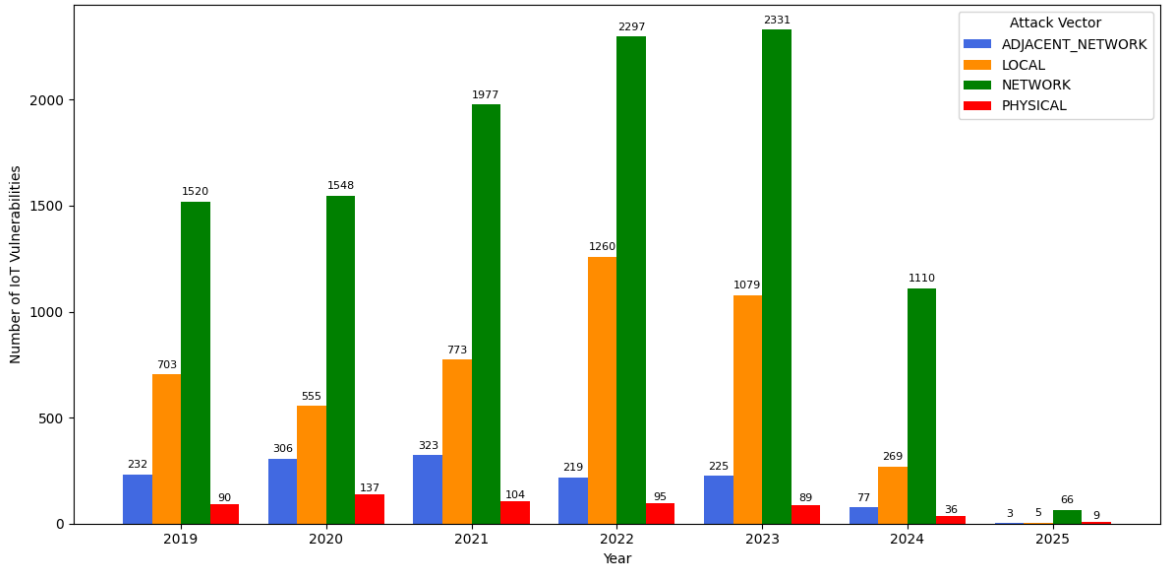


**FIGURE 5.1 : Répartition annuelle des vecteurs d'attaque dans l'IoT**

Les résultats montrent une domination claire du vecteur d'attaque réseau sur la période temporelle étudiée. Il représente la majorité des vulnérabilités chaque année, avec un pic de 2331 cas en 2023 , période marquée par une intensification des usages numériques liée à la pandémie de COVID-19. Cette tendance reflète la forte exposition des dispositifs IoT aux réseaux publics et internes. Cette prédominance s'explique par la nature même des objets connectés, conçus pour échanger en continu avec leur environnement via des protocoles tels que HTTP, MQTT, Telnet ou SSH. Cette connectivité permanente, essentielle à leur fonctionnement, augmente mécaniquement la surface d'exposition aux menaces extérieures [106], [107]. Un autre facteur réside dans la présence d' interfaces accessibles à distance , telles que les tableaux d'administration web, les interfaces de programmation applicative REST ou certains ports de maintenance, souvent mal protégés ou laissés ouverts par défaut. Selon plusieurs études, plus de 60 % des vulnérabilités répertoriées dans la base NVD concernent des services exposés sur Internet [106]. Des facteurs tels que des mots de passe faibles, l'absence de chiffrement ou des ports non restreints facilitent ainsi l'exploitation à distance, sans nécessiter

de contact physique [107]. La mauvaise gestion des mises à jour constitue aussi un facteur critique, car de nombreux appareils IoT restent non corrigés pendant de longues périodes , voire jamais. Ces failles persistantes sont alors exploitées par des botnets automatisés, tels que Mirai , Mozi ou Hajime , qui ciblent spécifiquement les services accessibles en réseau.

Enfin, contrairement aux vecteurs locaux ou physiques, qui nécessitent un accès direct au système cible, les attaques réseau peuvent être lancées à distance, à grande échelle et à faible coût . Cette facilité d'exécution explique pourquoi le vecteur réseau reste le moyen privilégié pour compromettre les dispositifs IoT [108].

En résumé, La prédominance du vecteur réseau dans l'IoT s'explique par la connectivité permanente des dispositifs, les interfaces souvent mal sécurisées et la gestion insuffisante des mises à jour . Ces facteurs rendent les appareils particulièrement vulnérables aux attaques à distance, souvent automatisées et faciles à déployer, faisant du vecteur réseau le moyen privilégié de compromission.

### 5.1.2 COMPLEXITÉ D'EXPLOITATION DES VULNÉRABILITÉS IOT

La complexité d'attaque constitue un facteur clé pour la classification des vulnérabilités, car elle permet d'évaluer le niveau de risque et la facilité d'exploitation d'une vulnérabililté. Cette évaluation repose sur le score CVSS v3, qui fournit une mesure standardisée de la sévérité des vulnérabilités. Le tableau 5.1 représente chaque niveau de gravité avec le scores CVSS correspondante et l'impact potentiel sur le système affecté.

| Niveau de gravité | Plage de score CVSS | Impact général |
|---|---|---|
| Faible | 0,1 – 3,9 | Faible impact, difficile à exploiter |
| Moyen | 4,0 – 6,9 | Exploitable avec impact limité |
| Haut | 7,0 – 8,9 | Sérieux, facilement exploitable, impact majeur |
| Critique | 9,0 – 10 | Très sévère, permet un contrôle complet |

**TABLEAU 5.1 : Catégorisation des vulnérabilités selon le score CVSS**

La figure 1.2 présente les statistiques issues de notre jeu de données, obtenues après un filtrage appliqué aux scores CVSS v3 de chaque vulnérabilité identifiée dans les appareils IoT collectés. Cette représentation permet d'observer la répartition des vulnérabilités selon leur niveau de sévérité mentionné dans le tableau précédent.

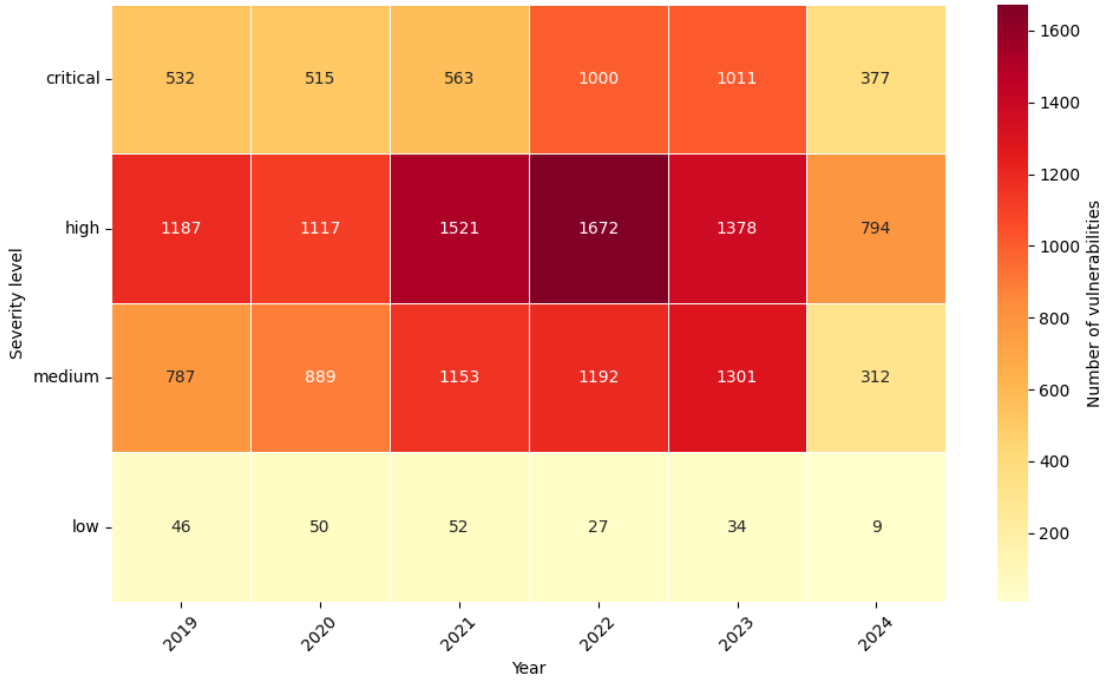


**FIGURE 5.2 : Répartition annuelle de la complexité des attaques dans l'IoT**

Les résultats montrent que la majorité des vulnérabilités ciblant les dispositifs IoT sont de gravité élevée ou critique, soulignant la nécessité d'une intervention immédiate

et priorisée. Cette situation est d'autant plus préoccupante que le nombre d'appareils IoT connectés augmente de manière exponentielle (Figure 5.3). Selon les données de Statista [109], le nombre total d'objets connectés devrait atteindre plusieurs dizaines de milliards dans les prochaines années, ce qui signifie que chaque vulnérabilité critique peut potentiellement affecter un très grand nombre de dispositifs simultanément.

L'augmentation massive des IoT crée un effet multiplicateur des risques : non seulement le nombre d'attaques potentielles augmente, mais la complexité de la gestion sécuritaire de cet écosystème s'accroît également. Les vulnérabilités de gravité faible ou moyenne restent relativement marginales dans ce contexte, mais même celles-ci peuvent devenir critiques si elles sont combinées avec des attaques automatisées ou des chaînes de dispositifs interconnectés. Ainsi, la croissance rapide des IoT transforme chaque faille critique en un vecteur majeur de compromission à grande échelle, rendant impératif le renforcement des mesures de sécurité, la mise à jour régulière des dispositifs, et la priorisation des vulnérabilités les plus dangereuses.

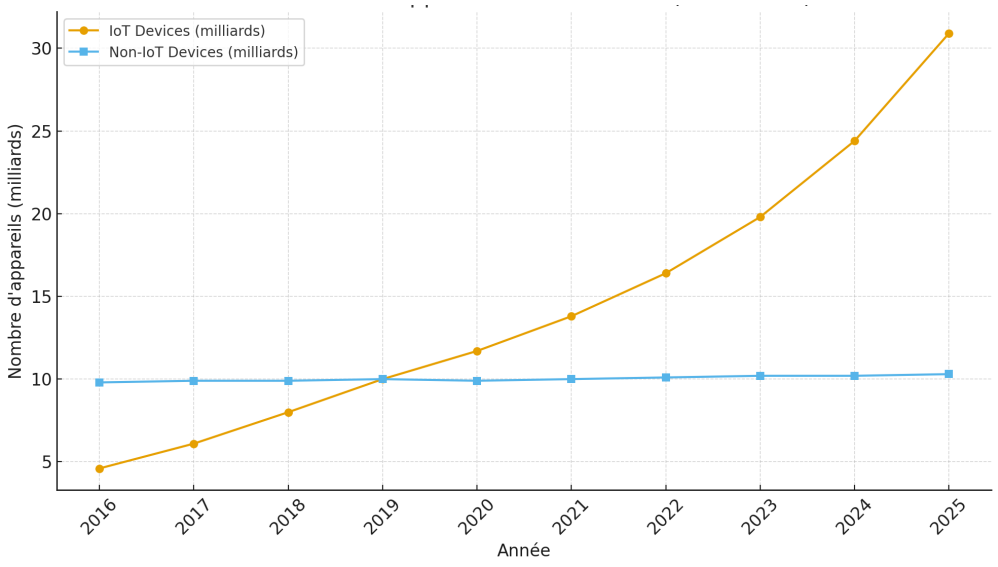


**FIGURE 5.3 : Évolution des appareils IoT et non-IoT (2016–2025) [109]**

En résumé, la corrélation entre l'augmentation des vulnérabilités IoT et la gravité des failles identifiées souligne que la sécurité des objets connectés dépasse désormais un simple enjeu technique. Elle constitue un facteur stratégique essentiel pour la protection globale des systèmes numériques.

### 5.1.3 ATTAQUES FRÉQUENTES PAR CATÉGORIE

Identifier les catégories de dispositifs IoT les plus vulnérables est essentiel pour orienter efficacement les stratégies de cybersécurité. La figure ci-dessous présente les catégories les plus exposées selon les données collectées.

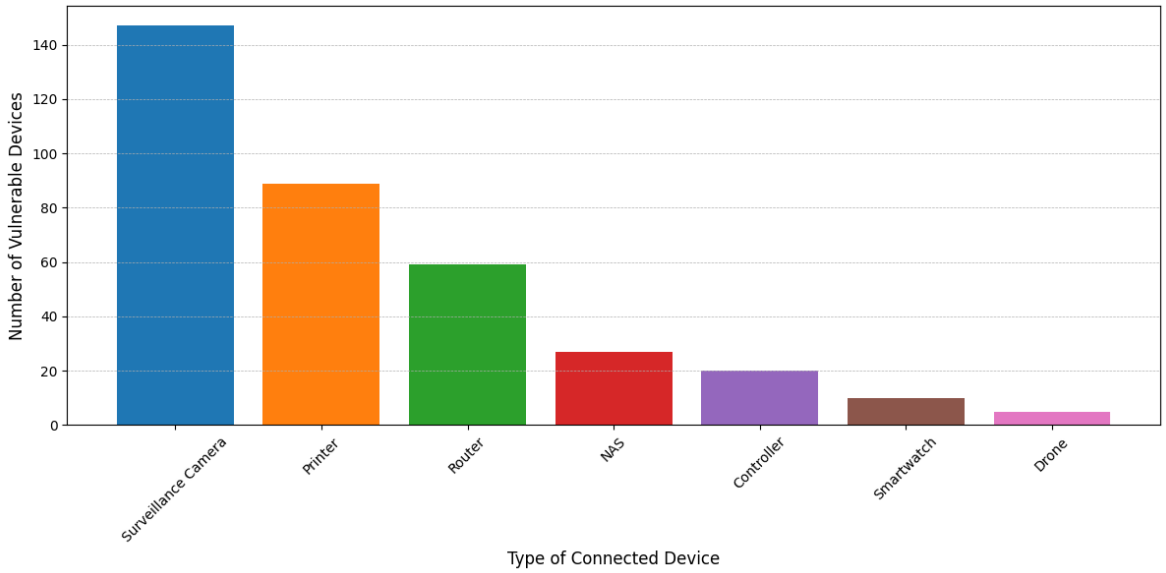


**FIGURE 5.4 : Nombre de dispositifs IoT vulnérables par catégorie (2019-2024)**

La Figure 5.4 montre une surreprésentation claire des vulnérabilités dans les caméras de surveillance, confirmant leur statut de cible principale dans l'écosystème IoT. Plusieurs études [110] indiquent que ces dispositifs souffrent fréquemment de micrologiciels propriétaires

obsolètes, de ports ouverts exposés et de mots de passe par défaut rarement modifiés. Ces faiblesses facilitent leur intégration dans des botnets de grande ampleur tels que Mirai. Les imprimantes et routeurs se classent respectivement deuxième et troisième. Ces équipements sont fréquemment négligés dans les politiques de gestion des correctifs [111], malgré leur rôle stratégique dans le traitement des données sensibles. L'exploitation de vulnérabilités sur ces appareils peut permettre des attaques de déplacement latéral à travers tout le réseau. Les NAS, contrôleurs, montres connectées et drones semblent moins affectés selon les données disponibles, bien que le risque réel puisse être sous-estimé.

Une analyse sectorielle a été réalisée afin d'identifier les secteurs les plus touchés par les vulnérabilités des dispositifs IoT. Les résultats, présentés dans la figure Figure 5.5, permettent de visualiser les niveaux de vulnérabilité relatifs et la répartition des appareils connectés dans chaque secteur.

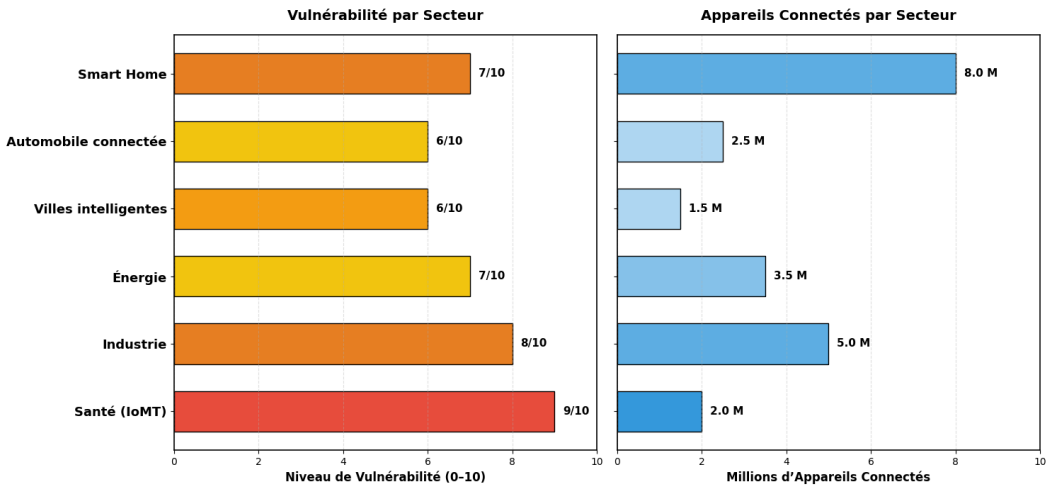


**FIGURE 5.5 : Distribution sectorielle des risques et du volume d'appareils connectés**

Les résultat par secteurs montre que la vulnérabilité et le nombre d'appareils varient selon les catégories. La Santé (IoMT) et le secteur industriel sont les plus exposés, en raison

de la criticité de leurs systèmes, de l'importance des données traitées et de l'interconnexion des dispositifs [59]. La Smart Home , qui compte le plus grand nombre de dispositifs, présente une vulnérabilité modérée, mais le risque global reste élevé à cause du volume d'appareils. Les secteurs de l'énergie, des villes intelligentes et de l'automobile connectée affichent des vulnérabilités modérées, mais restent exposés en raison de la criticité et de l'interconnexion de leurs systèmes. Ces résultats mettent en évidence la nécessité de renforcer la sécurité des dispositifs IoT , particulièrement dans les secteurs les plus sensibles.

### 5.1.4 VULNÉRABILITÉS CRITIQUES PAR FOURNISSEUR

La Figure 5.6 présente une analyse comparative des principaux fournisseurs IoT, fondée sur deux indicateurs clés : le nombre d'appareils connectés exposés (vulnérables) et le nombre moyen annuel de vulnérabilités critiques signalées.

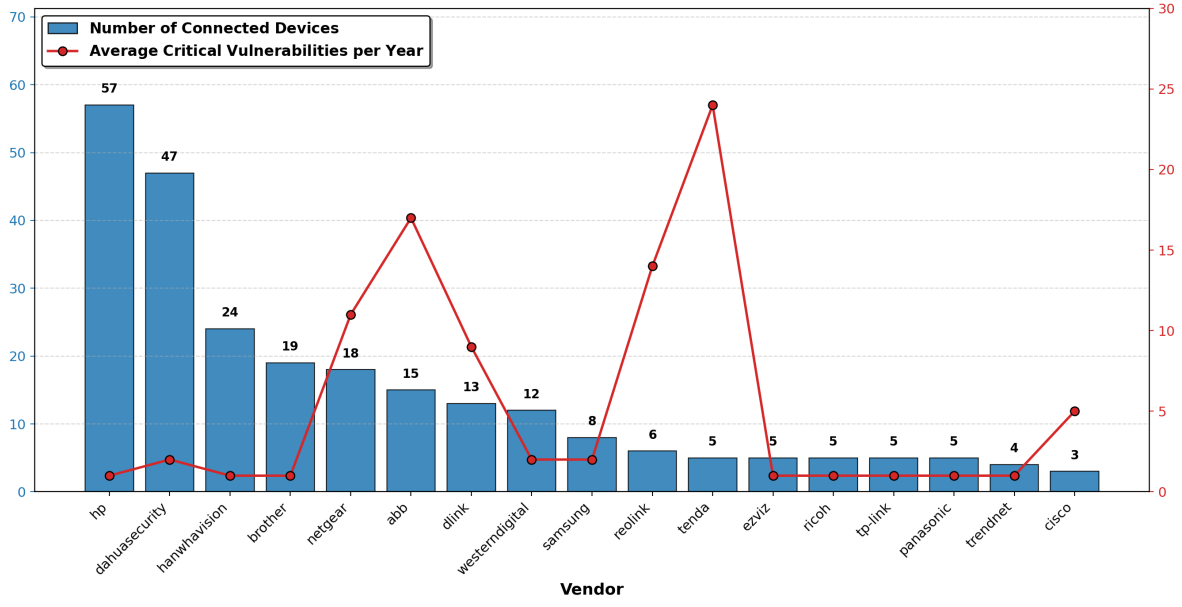


**FIGURE 5.6 : Exposition et vulnérabilités critiques des appareils IoT chez les fournisseurs**

Les résultats mettent en évidence un déséquilibre notable entre le nombre d'appareils exposés et la gravité des failles détectées. Par exemple, HP enregistre le plus grand nombre d'appareils vulnérables, tout en présentant une moyenne relativement faible de vulnérabilités critiques. Cela suggère que ses produits sont principalement affectés par des failles de gravité faible à modérée, ayant un impact limité sur la sécurité globale. À l'inverse, des fournisseurs tels que Tenda et ABB disposent d'un nombre restreint d'appareils vulnérables, mais concentrent une proportion élevée de vulnérabilités critiques. Cette forte densité de failles graves sur un petit nombre de produits traduit un niveau de risque supérieur et révèle des faiblesses potentielles au niveau de la sécurité logicielle, de la gestion des mises à jour ou des configurations par défaut.

Les résultats montrent ainsi que le volume d'appareils vulnérables ne constitue pas un indicateur suffisant pour évaluer le niveau de sécurité d'un fournisseur. Une évaluation plus fiable du risque nécessite une analyse conjointe du nombre d'appareils affectés et de la sévérité des vulnérabilités associées.

### 5.1.5 PRODUITS IOT À HAUT RISQUE

Dans cette partie, nous analysons les dix produits IoT présentant la moyenne annuelle la plus élevée de vulnérabilités critiques signalées. Les résultats révèlent une forte disparité entre les dispositifs, illustrant des niveaux d'exposition et de robustesse hétérogènes selon le fabricant et la catégorie d'appareil.

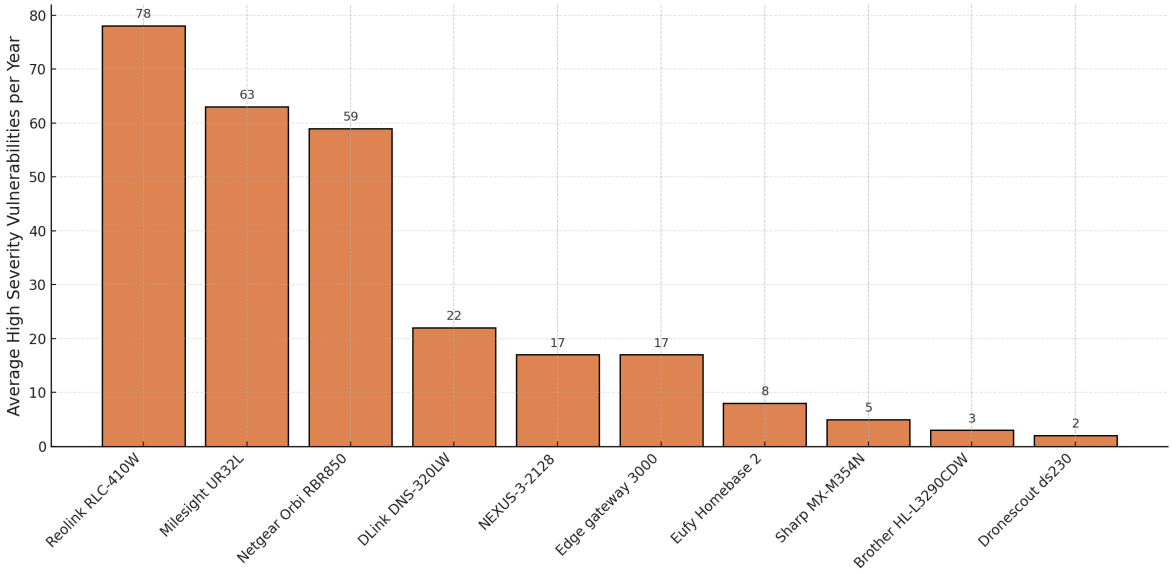


**FIGURE 5.7 : Top 10 des appareils IoT selon la moyenne annuelle des vulnérabilités critiques**

L'analyse met en évidence une concentration élevée de vulnérabilités critiques dans certaines catégories d'appareils IoT. La caméra IP Reolink RLC-410W présente une moyenne annuelle de 78 vulnérabilités critiques, suivie par la passerelle industrielle Milesight UR32L avec 63 et le routeur Netgear Orbi RBR850 avec 59. Ces résultats indiquent que les appareils de surveillance et les composants d'infrastructure réseau figurent parmi les plus exposés aux menaces de sécurité de haute gravité [112].

### 5.1.6 TYPE D'ATTAQUES LES PLUS FRÉQUENTES

La Figure 5.8 illustre la distribution des types de vulnérabilités les plus fréquemment signalées dans les appareils IoT entre 2019 et 2024, selon les données agrégées de la base CVE.

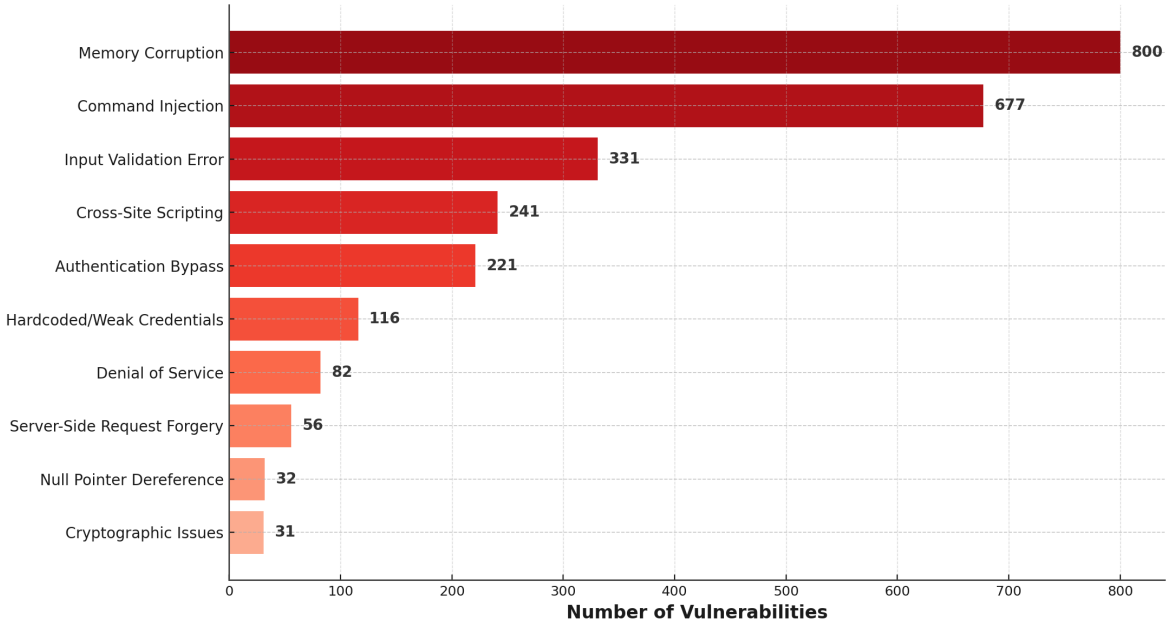


**FIGURE 5.8 : Distribution des types de vulnérabilités les plus fréquentes dans les appareils IoT (2019–2024)**

Les résultats révèlent une forte prédominance de trois types de vulnérabilités dans les objets connectés : la corruption de mémoire (800 occurrences), l' injection de commandes (677 occurrences) et les erreurs de validation des entrées (331 occurrences). Cette concentration s'explique principalement par les contraintes inhérentes aux appareils IoT, telles que la mémoire limitée, les ressources matérielles limitées et les composants simplifiés, qui favorisent l'usage de firmwares développés en C/C++ [113], souvent dépourvus de protections modernes de la mémoire et de mécanismes rigoureux de validation des entrées. Ainsi, ces vulnérabilités fondamentales demeurent à la fois fréquentes et critiques, car elles sont faciles à exploiter dans des environnements IoT peu sécurisés et rarement mis à jour. En revanche, d'autres types de failles, telles que les erreurs cryptographiques, les attaques par déni de service ou les tentatives d'accès à une adresse inexistante, sont moins courants.

La Figure 5.9 présente la distribution des types d'attaques les plus fréquentes pour chaque catégorie d'appareil IoT.


**FIGURE 5.9 : Distribution des types d'attaques fréquentes selon les catégories d'appareils IoT**

L'analyse de cette distribution montre que les types d'attaques dominants varient considérablement selon les catégories d'appareils, reflétant des vulnérabilités structurelles spécifiques à chaque famille d'objets connectés. Cette hétérogénéité met en évidence la diversité des profils de risque au sein de l'écosystème IoT et souligne l'importance d'adopter des stratégies de cybersécurité différenciées, adaptées aux caractéristiques techniques et fonctionnelles de chaque type d'appareil.

## 5.2 TEMPS DE REMÉDIATION PAR FOURNISSEUR (RQ2)

Le temps de réponse des fournisseurs constitue un indicateur clé de leur maturité en cybersécurité. Un délai long prolonge la période pendant laquelle les systèmes restent exposés aux risques et peut contraindre les entreprises dans la manière dont elles déploient ou

utilisent certaines technologies. Cette mesure est donc essentielle pour évaluer la réactivité des fournisseurs et guider les choix d'équipements, notamment dans le domaine des dispositifs IoT. L'importance de ce facteur se manifeste notamment dans le choix du fournisseur pour le déploiement de dispositifs IoT, en particulier dans le domaine de la vidéosurveillance. En 2021, plusieurs organisations équipées de caméras de sécurité *Verkada* ont été épargnées par une vague d'attaques massives exploitant des vulnérabilités présentes dans des produits concurrents tels que ceux de *Dahua* et *Hikvision*. Ces marques étaient particulièrement ciblées en raison de failles connues, notamment la présence d'interfaces d'administration accessibles depuis Internet et l'usage persistant d'identifiants par défaut [114]. À l'inverse, les dispositifs *Verkada* intégraient une authentification à double facteur, un chiffrement bout à bout des flux vidéo et un mécanisme de mise à jour automatique du micrologiciel, réduisant ainsi considérablement leur surface d'attaque. Lorsque le botnet *Mirai* et ses variantes ont compromis des milliers de caméras IP vulnérables, les systèmes protégés par ces politiques de sécurité intégrées n'ont subi aucun impact.Le scénario d'attaque complet, depuis la tentative d'infection du produit Hikvision jusqu'au déploiement de Moobot, est illustré dans la Figure 5.10 :

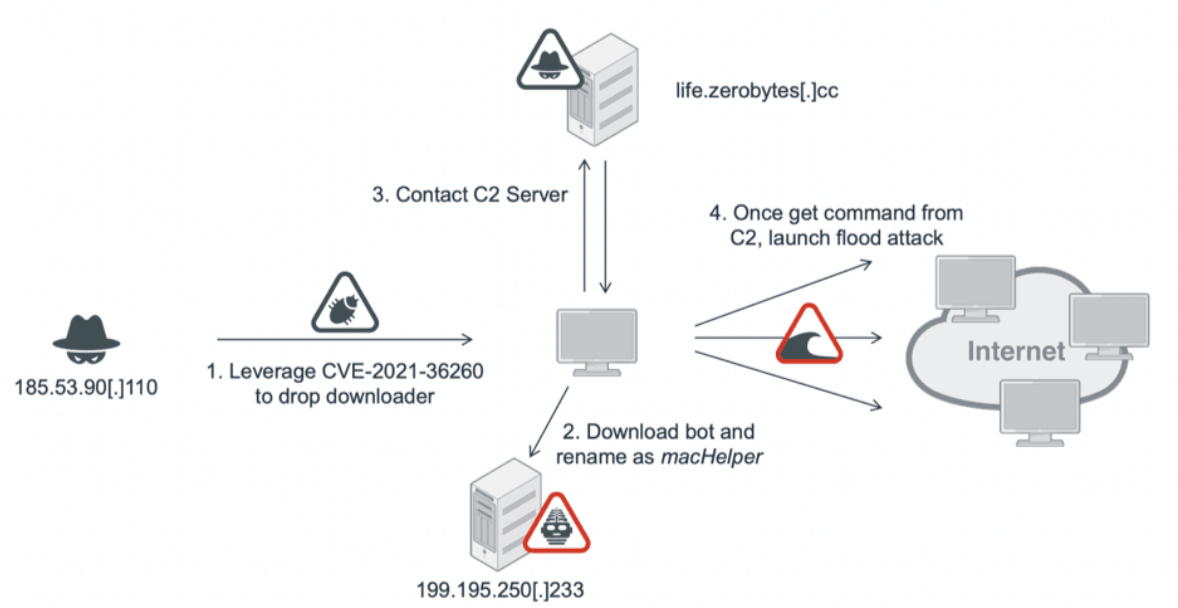


**FIGURE 5.10 : Scénario d'attaque cible la vulnérabilité Hikvision [114]**

Cet exemple illustre qu'un choix éclairé de produit IoT, fondé sur la maturité du fournisseur et la disponibilité de correctifs réguliers, peut constituer une barrière déterminante contre des attaques automatisées à grande échelle. Cependant, malgré l'importance stratégique de cette métrique, il n'existe actuellement aucun mécanisme structuré et automatisé permettant d'évaluer le temps moyen de correction des vulnérabilités par fournisseur. Cette absence limite la capacité à comparer objectivement les pratiques de gestion des vulnérabilités et à évaluer la réactivité des fournisseurs face aux menaces. Dans cette section, nous présentons les résultats obtenus en appliquant notre approche méthodologique pour le calcul du temps moyen de remédiation des vulnérabilités par fournisseur.

### 5.2.1 RÉSULTATS COMPARATIFS DE L'APPROCHE PROPOSÉE

Comme indiqué dans la section méthodologie, le champ `dateReserved` a été retenu comme le proxy le plus pertinent pour représenter la date réelle de découverte. Ce choix a été

justifié par une étude comparative effectuée entre différentes dates afin d'identifier celle la plus proche de la réalité. Une analyse empirique a ensuite permis de constater un écart médian de 27 jours par rapport aux dates de découverte officiellement rapportées. Cet écart est ainsi appliqué comme facteur de correction dans le calcul du temps de remédiation.

Nous avons appliqué notre méthode d'estimation du temps de remédiation à un ensemble de fournisseurs. La sélection des fournisseurs a été guidée par les données disponibles dans la base ZDI, qui fournit des dates précises liées aux temps de remédiation et pour lesquelles des données comparatives étaient accessibles. Deux critères principaux ont été retenus pour cette sélection : l'importance des fournisseurs sur le marché et la fréquence de leurs vulnérabilités rapportées dans la base ZDI.Les résultats de la comparaison sont présentés dans le tableau suivant :

| **Fournisseur** | **Gravité** | **ZDI (jours)** | **Notre estimation (jours)** |
|---|---|---|---|
| Canon | Élevée | 46 | 44 |
| Samsung | Élevée | 129 | 83 |
| Google | Élevée | 127 | 122 |
| HP | Élevée | 91 | 88 |
| NVIDIA | Élevée | 118 | 162 |
| Samsung | Moyenne | 129 | 123 |
| Cisco | Moyenne | 198 | 197 |
| Apple | Moyenne | 67 | 37 |

**TABLEAU 5.2 : Comparaison des temps moyens de remédiation par fournisseur**

Les résultats montrent que, pour un ensemble représentatif de fournisseurs IoT bien connus et pour différents niveaux de gravité, notre méthode produit des estimations de temps de remédiation globalement cohérentes avec celles rapportées par la ZDI. Les écarts observés peuvent s'expliquer par des variations individuelles entre la date de réservation CVE et la date réelle de découverte des différences que le facteur de correction médian ne peut pas complètement compenser dans tous les cas.

Ces résultats montrent également que la date de réservation d'une vulnérabilité peut être considérée comme un proxy fiable de sa date de signalement, avec un écart médian empirique de 27 jours. Cet écart temporel reste dans une marge d'erreur raisonnable, susceptible de varier selon le jeu de données analysé.

## 5.3 PRÉDICTION PROACTIVE DES VULNÉRABILITÉS IOT (RQ3)

La croissance continue des vulnérabilités publiées affectant les dispositifs IoT souligne la nécessité urgente de passer d'une approche réactive à une approche prédictive en cybersécurité. Les solutions actuelles se concentrent principalement sur l'analyse de vulnérabilités déjà connues, sans offrir de mécanismes permettant d'anticiper celles à venir. Cette étude explore l'utilisation de modèles d'apprentissage supervisé afin d'estimer, à partir des tendances historiques, la probabilité qu'une vulnérabilité affectant un dispositif IoT apparaisse dans une fenêtre temporelle future de $N$ jours.

L'objectif est de sélectionner le modèle le plus adapté à cette tâche , en s'appuyant sur des données accessibles au grand public. Pour cela, nous avons examiné les principaux modèles de classification employés dans ce contexte. Les approches étudiées appartiennent à trois grandes familles : les modèles classiques d'apprentissage supervisé , les modèles d'apprentissage profond , et les modèles issus du traitement du langage naturel (NLP) . Chaque modèle repose sur des fondements mathématiques spécifiques , détaillés dans les sections suivantes.

### 5.3.1 MODÈLES CLASSIQUES

Un modèle de classification est un algorithme d'apprentissage supervisé dont le but est d'associer une observation $x \in \mathbb{R}^n$ à une étiquette $y$ appartenant à un ensemble fini de classes $\mathscr{Y} = \{c_1, c_2, \ldots, c_k\}$ [62]. Ce modèle apprend, à partir d'un ensemble de données annotées

$\mathscr{D} = \{(x_i, y_i)\}_{i=1}^{N}$, une *fonction de décision* :

$$f : \mathbb{R}^n \to \mathscr{Y}$$

ou, de manière probabiliste, une *fonction d'estimation* :

$$f(x) = \arg\max_{y \in \mathscr{Y}} P(y \mid x)$$

où $P(y \mid x)$ représente la probabilité qu'une instance $x$ appartienne à la classe $y$.

L'apprentissage consiste à minimiser une *fonction de perte* $L(f(x_i), y_i)$ mesurant l'écart entre la classe prédite et la classe réelle sur l'ensemble des exemples d'entraînement. Sur le plan conceptuel, les modèles de classification permettent de détecter et de généraliser les régularités présentes dans les données afin de prendre des décisions automatiques sur de nouveaux cas.Dans le cadre de la prédiction de vulnérabilités, ils permettent d'apprendre les relations entre les caractéristiques historiques observées et la probabilité d'apparition future d'un événement [104]. Leur flexibilité réside dans la possibilité d'intégrer des variables dérivées du temps, ce qui leur confère une capacité d'anticipation sans nécessiter de modèles séquentiels complexes.

**RÉGRESSION LOGISTIQUE**

La régression logistique est un modèle linéaire de classification supervisée qui estime la probabilité qu'une observation appartienne à une classe donnée [23]. Dans cette étude, elle permet de prédire la survenue d'une vulnérabilité dans les 7 jours suivants , comme présenté dans la partie méthodologie.Elle se définit par la formule :

$$P(y = 1 \mid x) = \sigma(w^T x + b) = \frac{1}{1 + e^{-(w^T x + b)}}$$

où $w$ est le vecteur des poids du modèle et $b$ le biais. La fonction sigmoïde $\sigma(\cdot)$ transforme la combinaison linéaire des caractéristiques en une probabilité comprise entre 0 et 1.

Dans le cadre de données temporelles, chaque vecteur $x_t$ dans notre étude prend une valeur binaire, indiquant la présence ou l'absence d'une vulnérabilité dans les 7 jours précédents, en lien avec la vulnérabilité ciblée. Le modèle apprend ainsi à associer ce pattern passé à la probabilité d'apparition d'une vulnérabilité dans la fenêtre des 7 jours suivants. L'apprentissage se fait en minimisant la fonction de perte par entropie croisée[23] :

$$L = -\frac{1}{N} \sum_{i=1}^{N} \left[ y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i) \right]$$

où $y_i$ est la classe réelle et $\hat{y}_i = P(y_i = 1 \mid x_i)$ est la probabilité prédite. L'optimisation est généralement réalisée par descente de gradient, qui ajuste les poids $w$ et le biais $b$ pour améliorer la précision de prédiction.

**SUPPORT VECTOR MACHINE (SVM)**

Le Support Vector Machine (SVM) est un modèle de classification supervisée qui cherche à séparer les classes en trouvant un hyperplan [115], Dans notre étude, chaque observation correspond à un vecteur binaire $x_t$ indiquant la présence ou l'absence d'une vulnérabilité dans les 7 jours précédents, et le modèle prédit si une vulnérabilité apparaîtra dans les 7 jours suivants.La fonction de décision du SVM peut s'écrire simplement :

$$f(x) = w^T x + b$$

où $w$ est le vecteur des poids et $b$ le biais. Le modèle classe une observation comme vulnérable si $f(x) \geq 0$, et non vulnérable sinon. L'hyperplan correspond à la frontière $f(x) = 0$ qui sépare les classes.Dans le cadre de données temporelles, le SVM utilise les informations binaires des 7 jours précédents pour apprendre une frontière qui permet de prédire si une vulnérabilité apparaîtra ou non dans les 7 jours suivants.

**RANDOM FOREST ET XGBOOST**

Random Forest et XGBoost sont des modèles basés sur des ensembles d'arbres de décision[24] [25]. Ces méthodes construisent plusieurs arbres pour améliorer la précision et la robustesse des prédictions. Dans le cas du Random Forest, plusieurs arbres sont entraînés sur des sous-échantillons aléatoires des données (bootstrap) et la prédiction finale est obtenue par vote majoritaire :

$$\hat{y} = \text{mode}\{h_1(x), h_2(x), \ldots, h_T(x)\}$$

où $h_t(x)$ est la prédiction de l'arbre $t$ et $T$ est le nombre total d'arbres.

Le XGBoost améliore les performances en construisant les arbres de manière séquentielle, chaque nouvel arbre corrigeant les erreurs des arbres précédents :

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + \eta f_t(x_i)$$

où $\eta$ est le taux d'apprentissage et $f_t$ est l'arbre ajouté à l'itération $t$. L'objectif global du modèle réunit deux éléments : la perte sur les prédictions et une pénalité qui limite la complexité des arbres :

$$L^{(t)} = \sum_{i=1}^{N} l(y_i, \hat{y}_i^{(t)}) + \sum_{t} \Omega(f_t)$$

Dans notre jeu de données temporel, chaque vecteur $x_t$ indique la présence ou l'absence d'une vulnérabilité au cours des sept jours précédents. Les modèles *Random Forest* et *XGBoost* utilisent ces motifs pour prédire la survenue d'une vulnérabilité dans les sept jours suivants, en capturant à la fois les relations simples et complexes entre les observations passées.

### 5.3.2 MODÈLES D'APPRENTISSAGE PROFOND

L'apprentissage profond, est une branche de l'apprentissage automatique qui utilise des réseaux de neurones composés de plusieurs couches pour apprendre automatiquement des représentations complexes des données et modéliser des relations non linéaires. Plusieurs architectures de réseaux de neurones ont été développées dans le cadre du deep learning, chacune adaptée à des types de données et d'objectifs spécifiques. Parmi les plus courantes les réseaux récurrents et leurs variantes comme le LSTM pour les données séquentielles, ainsi que les modèles de type Transformer utilisés dans le traitement du langage naturel (NLP).

#### RÉSEAU LSTM (LONG SHORT-TERM MEMORY).

Le réseau LSTM (Long Short-Term Memory) est une extension des réseaux de neurones récurrents (RNN) conçue pour pallier le problème de l'oubli à long terme dans le traitement de données séquentielles intègre un mécanisme de mémoire interne qui lui permet de conserver

et de mettre à jour les informations pertinentes au fil du temps grâce à des portes de contrôle [26]. Le fonctionnement d'une cellule LSTM est défini par les équations suivantes :

$$
\begin{aligned}
i_t &= \sigma(W_i x_t + U_i h_{t-1} + b_i) \\
f_t &= \sigma(W_f x_t + U_f h_{t-1} + b_f) \\
o_t &= \sigma(W_o x_t + U_o h_{t-1} + b_o) \\
\tilde{c}_t &= \tanh(W_c x_t + U_c h_{t-1} + b_c) \\
c_t &= f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \\
h_t &= o_t \odot \tanh(c_t)
\end{aligned}
$$

Ces mécanismes de portes d'entrée ($i_t$), d'oubli ($f_t$) et de sortie ($o_t$) permettent au modèle de réguler le flux d'information et de maintenir une mémoire sélective des états passés[26]. Dans le contexte de l'analyse temporelle des vulnérabilités d'un produit, le réseau LSTM peut être utilisé pour modéliser l'évolution des événements dans le temps. Chaque entrée du réseau correspond à une observation temporelle comme le nombre de vulnérabilités détectées à une date donnée ou les caractéristiques associées à chaque événement. Le LSTM reçoit ces séquences ordonnées chronologiquement et apprend à relier les états passés aux comportements futurs, en ajustant ses portes internes pour conserver les informations pertinentes sur plusieurs pas de temps. Ce mécanisme lui permet d'identifier des tendances d'évolution, des cycles récurrents ou encore des périodes d'accumulation de vulnérabilités.

### 5.3.3 MODÈLES NLP

Le NLP désigne l'ensemble des méthodes et modèles de l'intelligence artificielle dédiés à l'analyse et au traitement automatique du langage naturel. Parmi ces modèles, les architectures de type Transformer, initialement conçues pour le traitement séquentiel du langage naturel,

reposent sur un mécanisme d'attention qui permet de pondérer l'importance relative de chaque élément d'une séquence par rapport aux autres, sans contrainte de position fixe dans le temps [116] :

$$\text{Attention}(Q,K,V) = \text{softmax}\left(\frac{QK^\top}{\sqrt{d_k}}\right)V$$

Dans le cadre de cette étude, nous avons généré des données textuelles à partir des informations disponibles sur les vulnérabilités, en combinant les dates, les descriptions et les types d'incidents. Cette représentation enrichie permet au Transformer d'apprendre plus efficacement, en exploitant à la fois les caractéristiques temporelles et sémantiques de chaque événement. Le modèle est ainsi capable de modéliser les dépendances entre incidents passés et futurs et d'identifier automatiquement les périodes ou les occurrences les plus influentes dans la dynamique globale du produit.

**MODÈLES BERT**

Le modèle BERT repose sur le mécanisme d'auto-attention introduit par les architectures de type Transformer [113] :

$$\text{Attention}(Q,K,V) = \text{softmax}\left(\frac{QK^\top}{\sqrt{d_k}}\right)V$$

Cependant, BERT est bidirectionnel, ce qui lui permet de considérer le contexte à la fois avant et après chaque élément d'une séquence. Dans cette étude, où les données textuelles sont générées à partir de descriptions et de dates, ce mécanisme permet au modèle d'apprendre les relations contextuelles et temporelles complexes entre les événements, produisant ainsi des

représentations plus précises et adaptées à l'analyse des patterns spécifiques de notre jeu de données.

**MODÈLES LLAMA3**

LLaMA 3 est un modèle de langage basé sur une architecture de type Transformer, utilisé en traitement automatique du langage naturel (NLP). conçu pour modéliser efficacement les dépendances contextuelles à grande échelle et produire des représentations textuelles riches [117]. Son objectif principal est de comprendre et générer du texte de manière cohérente et précise à partir de vastes corpus. Selon notre jeu de données, LLaMA3 est exploité pour apprendre les relations complexes et temporelles présentes dans les données textuelles générées à partir de la concaténation des descriptions et des dates des vulnérabilités, tout en évaluant sa capacité d'apprentissage sur cet ensemble.

### 5.3.4 ANALYSE DES RÉSULTATS D'APPRENTISSAGE

L'étude repose sur la conception de deux jeux de données complémentaires, construits à partir des informations liées aux produits IoT extraites des bases CVE et NVD. La création de ces jeux de données tient compte de la capacité d'apprentissage propre à chaque famille de modèles. En effet, les modèles de classification exploitent principalement des données tabulaires, construites à partir de la date de publication, du score CVSS, du niveau de gravité et du nom du produit concerné. À l'inverse, les modèles de type NLP s'appuient sur une représentation textuelle de ces mêmes informations, obtenue en concaténant et en enrichissant les descriptions afin de former un texte cohérent décrivant la vulnérabilité. L'objectif de cette approche est d'exploiter la spécificité et la puissance de chaque modèle pour obtenir les meilleures performances possibles.

**JEU DE DONNÉES STRUCTURÉ**

Le premier jeu de données rassemble l'ensemble des informations quantitatives et catégorielles extraites des bases CVE et NVD, incluant pour chaque produit IoT les caractéristiques techniques, le niveau de sévérité, le type de vulnérabilité et la famille du produit concerné. Cette représentation permet de modéliser efficacement les relations entre les différentes variables et de capturer les tendances temporelles associées à l'apparition des vulnérabilités.

Chaque exemple du jeu d'entraînement est formalisé sous la forme d'un couple $(x_i, y_i)$, où $x_i$ désigne le vecteur de caractéristiques associé à un instant donné, et $y_i$ la classe cible représentant la survenue (ou non) d'une vulnérabilité dans la période suivante. Ainsi, le processus d'apprentissage cherche à approximer une fonction de décision :

$$f : \mathbb{R}^n \to Y,$$

ou, de manière probabiliste :

$$f(x) = \arg\max_{y \in Y} P(y \mid x),$$

où $P(y \mid x)$ représente la probabilité qu'une instance $x$ appartienne à la classe $y$. L'objectif est de minimiser une fonction de perte $L(f(x_i), y_i)$ mesurant l'écart entre la classe prédite et la classe réelle sur l'ensemble des exemples d'entraînement.

Ce jeu de données a servi à l'entraînement des modèles de classification traditionnels tels que la régression logistique, le SVM, le Random Forest et le XGBoost, qui exploitent efficacement les motifs temporels et les relations entre variables numériques.

**JEU DE DONNÉES TEXTUEL (NON STRUCTURÉ)**

Le second jeu de données a été conçu à partir des informations textuelles disponibles dans les descriptions des vulnérabilités, enrichies par la date de publication, le type d'incident et d'autres métadonnées pertinentes issues des bases CVE et NVD. Ces éléments ont été concaténés et prétraités (nettoyage, normalisation, encodage) afin de produire une représentation textuelle enrichie, adaptée aux modèles de traitement du langage naturel (NLP).

Les résultats d'apprentissage obtenus pour chacun des modèles présentés sont synthétisés dans le tableau 5.3, afin de comparer leurs performances respectives.

| Modèle | Classe | Précision | Rappel | F1-score |
|---|---|---|---|---|
| Random Forest | Pas de vulnérabilité (0) | 0.70 | 0.76 | 0.73 |
| | Vulnérabilité (1) | 0.88 | 0.92 | 0.90 |
| | **Exactitude** | | **88,4%** | |
| XGBoost | Pas de vulnérabilité (0) | 0.93 | 0.97 | 0.95 |
| | Vulnérabilité (1) | 0.96 | 0.92 | 0.94 |
| | **Exactitude** | | **94,5%** | |
| Logistic Regression | Pas de vulnérabilité (0) | 0.73 | 0.85 | 0.78 |
| | Vulnérabilité (1) | 0.93 | 0.90 | 0.91 |
| | **Exactitude** | | **89,2%** | |
| SVM | Pas de vulnérabilité (0) | 0.71 | 0.78 | 0.75 |
| | Vulnérabilité (1) | 0.91 | 0.92 | 0.91 |
| | **Exactitude** | | **89,8%** | |
| LSTM | Pas de vulnérabilité (0) | 0.79 | 0.80 | 0.79 |
| | Vulnérabilité (1) | 0.97 | 0.95 | 0.96 |
| | **Exactitude** | | **91,0%** | |
| MLP | Pas de vulnérabilité (0) | 0.66 | 0.84 | 0.74 |
| | Vulnérabilité (1) | 0.96 | 0.94 | 0.95 |
| | **Exactitude** | | **92,0%** | |
| BERT | Pas de vulnérabilité (0) | 0.82 | 0.63 | 0.64 |
| | Vulnérabilité (1) | 0.66 | 0.84 | 0.67 |
| | **Exactitude** | | **73,4%** | |
| LLaMA3 | Pas de vulnérabilité (0) | 0.64 | 0.70 | 0.67 |
| | Vulnérabilité (1) | 0.66 | 0.60 | 0.63 |
| | **Exactitude** | | **64,9%** | |

**TABLEAU 5.3 : Résultats comparatifs des modèles d'apprentissage automatique et profond.**

Les résultats montrent que l'algorithme XGBoost fournit les meilleures performances pour prédire les vulnérabilités à court terme des dispositifs IoT, atteignant une précision globale de 94,5%. Il se distingue par sa capacité équilibrée à détecter à la fois les jours vulnérables et non vulnérables, ce qui le rend particulièrement adapté à cette tâche.

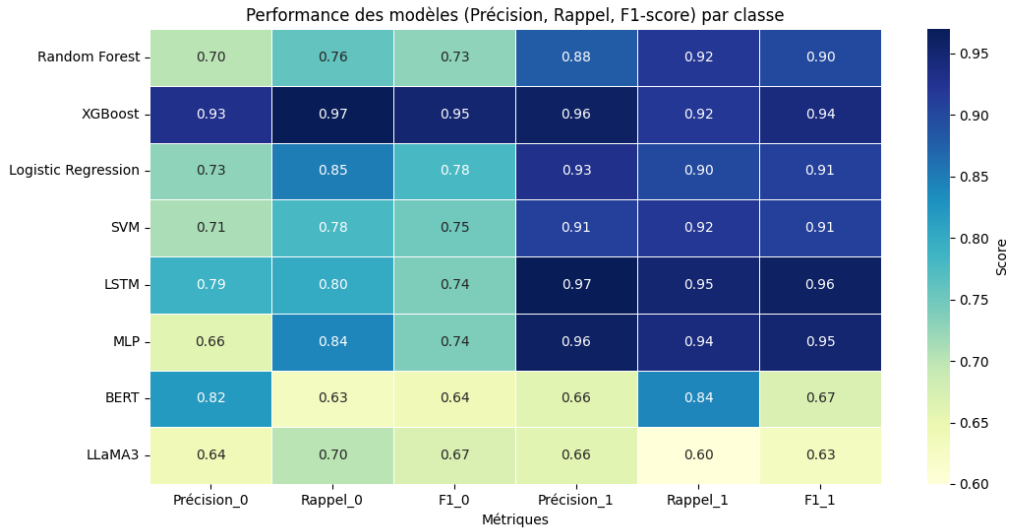


**FIGURE 5.11 : Comparaison des performances des modèles par classe**

D'autres modèles classiques, tels que Random Forest, SVM et la régression logistique, présentent également de bonnes performances, mais montrent un léger déséquilibre dans la détection des classes, favorisant parfois les cas positifs ou négatifs. Les modèles d'apprentissage profond, tels que LSTM et MLP, identifient efficacement les jours avec vulnérabilités, mais génèrent un nombre plus élevé de faux positifs, ce qui peut affecter leur fiabilité globale. Enfin, les modèles conçus pour le traitement du langage naturel, tels que BERT et LLaMA 3 montrent des performances inférieures aux modèles de classification et de gradient boosting. Bien que ces architectures soient optimisées pour traiter des données textuelles et capturer des dépendances contextuelles, elles restent limitées dans ce contexte en raison de la nature temporelle et structurée des événements de vulnérabilité.

## 5.4 DISCUSSION DES RÉSULTATS

Cette section discute les résultats obtenus au regard des trois questions de recherche et des choix méthodologiques présentés dans le chapitre précédent. L'objectif est d'interpréter les tendances observées, de mettre en perspective les résultats empiriques et d'expliquer les écarts éventuels par rapport aux travaux existants, afin de mieux comprendre le comportement des vulnérabilités, les mécanismes de remédiation et le potentiel des approches prédictives dans l'écosystème IoT.

### 5.4.1 DISCUSSION DES TENDANCES DES VULNÉRABILITÉS IOT (RQ1)

Les résultats montrent une domination nette du vecteur d'attaque réseau sur l'ensemble de la période 2019-2024. Cette observation est cohérente avec la nature même des dispositifs IoT, dont la valeur d'usage repose sur une connectivité permanente et sur l'exposition d'interfaces d'administration, d'API ou de services de maintenance accessibles à distance. Dans ce contexte, l'attaque à distance présente un rapport coût/impact particulièrement favorable pour les attaquants : elle est scalable, automatisable (scans, exploitation opportuniste), et ne requiert ni accès physique ni proximité réseau. Ainsi, la prédominance du vecteur réseau confirme que l'IoT constitue un environnement structurellement exposé, où la surface d'attaque dépend davantage de la connectivité et des services exposés que de l'usage local du dispositif.L'analyse par sévérité met en évidence une proportion importante de vulnérabilités classées à impact élevé ou critique. Deux interprétations complémentaires peuvent être avancées. D'une part, une partie des dispositifs IoT (caméras, routeurs, passerelles industrielles) implémente des services réseau sensibles (authentification, traitement de requêtes, exposition web) dans des environnements contraints, souvent avec des firmwares en C/C++ et des mécanismes de protection limités. D'autre part, un biais de divulgation est possible : les vulnérabilités publiées et attribuées à des produits IoT sont fréquemment celles jugées les plus exploitables ou les

plus impactantes, ce qui peut surreprésenter la criticité par rapport à l'ensemble des failles réellement présentes. Dans tous les cas, ces résultats confirment l'importance de prioriser les vulnérabilités à fort impact dans les politiques de sécurité IoT.

La distribution par catégories de dispositifs met en évidence une exposition particulièrement élevée des caméras de surveillance, suivies des imprimantes et des routeurs. Cette hiérarchie s'explique par la combinaison de plusieurs facteurs : la large diffusion de ces équipements, leur forte exposition au réseau (interfaces web, protocole de diffusion en temps réel, services d'administration à distance) et des pratiques de sécurité historiquement insuffisantes, telles que l'utilisation d'identifiants par défaut, des politiques de mise à jour irrégulières ou le recours à des composants logiciels obsolètes.L'analyse sectorielle révèle par ailleurs que les domaines de la santé (IoMT) et de l'industrie concentrent un niveau de risque élevé, en raison de la criticité des actifs concernés, de la longue durée de vie des équipements et des contraintes opérationnelles qui retardent l'application des correctifs de sécurité.À l'inverse, les dispositifs de la maison intelligente présentent une vulnérabilité moyenne à l'échelle individuelle, mais un risque global potentiellement important du fait du volume très élevé de dispositifs déployés. Dans ce contexte, même des vulnérabilités d'impact modéré peuvent entraîner des conséquences significatives à grande échelle, telles que la constitution de réseaux de machines zombies, la compromission du réseau domestique ou l'extraction non autorisée de données.

Enfin, l'analyse par type de vulnérabilité montre une prédominance de la corruption mémoire, de l'injection de commandes et des erreurs de validation des entrées. Ce résultat est cohérent avec les architectures logicielles des dispositifs IoT, où la surface d'attaque inclut fréquemment des analyseurs syntaxiques, des interfaces web et des composants chargés de l'interprétation des commandes. La persistance de ces familles de failles suggère que les efforts de sécurisation doivent cibler prioritairement la validation des entrées, la limitation des

privilèges, l'isolement des composants critiques et l'intégration de pratiques de développement sécurisé adaptées aux micrologiciels, telles que les tests par injection de données aléatoires, la revue de code et la compilation avec mécanismes de protection.

### 5.4.2 DISCUSSION DE L'ESTIMATION DU TEMPS DE REMÉDIATION (RQ2)

Les résultats comparatifs avec la ZDI montrent que l'utilisation de la date de réservation comme proxy de la découverte, corrigée par un décalage médian, produit des estimations globalement cohérentes. Cette cohérence suggère que, malgré l'absence fréquente de dates de découverte explicites dans les sources publiques, il est possible de construire une mesure reproductible et comparable entre fournisseurs à grande échelle. L'intérêt principal de cette approche est sa scalabilité : elle peut être appliquée à des milliers de vulnérabilités sans dépendre d'une analyse complexe de pages web hétérogènes ni d'un accès à des données privées. Les écarts observés entre l'estimation et les valeurs ZDI peuvent s'expliquer par plusieurs phénomènes. Premièrement, la relation entre dateReserved et la date réelle de découverte varie selon les pratiques des acteurs (éditeurs, chercheurs) : certaines vulnérabilités sont réservées très tôt, d'autres plus tard, et le délai dépend du processus de coordination. Deuxièmement, les fournisseurs publient parfois des correctifs avant la divulgation officielle ou, inversement, des correctifs peuvent être disponibles sans être clairement datés dans les sources publiques, ce qui perturbe l'alignement entre « correction effective » et « date publique ». Troisièmement, la ZDI ne couvre pas uniformément tous les fournisseurs ni tous les types de vulnérabilités : la comparabilité dépend donc du sous-ensemble commun de données.

Sur le plan de l'interprétation, un temps de remédiation moyen plus faible peut refléter une maturité élevée (processus de triage, mises à jour fréquentes, pipelines de patch), mais il doit être interprété avec prudence : la valeur moyenne peut masquer une forte variabilité, et certains fournisseurs peuvent corriger rapidement les vulnérabilités médiatisées tout en

retardant des failles moins visibles. Ainsi, une approche plus robuste consiste à analyser, en complément de la moyenne, la médiane et des courbes de survie, afin de mieux caractériser la distribution des délais de correction et d'éviter des conclusions fondées uniquement sur des valeurs agrégées.

### 5.4.3 DISCUSSION DES PERFORMANCES PRÉDICTIVES (RQ3)

Les résultats de classification montrent que XGBoost obtient les meilleures performances globales, ce qui est cohérent avec la littérature portant sur des données tabulaires enrichies par des caractéristiques temporelles. En effet, les modèles d'amplification par gradient exploitent efficacement les relations non linéaires, les interactions entre variables et les seuils décisionnels, tout en restant relativement robustes face au bruit.Dans un cadre temporel où les observations sont discrétisées en fenêtres régulières et représentées par des variables dérivées du temps (présence, fréquence ou accumulation d'événements sur une période donnée), ce type de modèle est capable de capturer des motifs de récurrence, des effets d'accumulation et des périodes à risque, sans recourir à une modélisation séquentielle explicite.

Afin de compléter l'analyse fondée sur les métriques classiques (précision, rappel et F1-score), nous introduisons un score de confiance visant à évaluer la stabilité et la cohérence globale des prédictions produites par chaque modèle. Le tableau 5.4 présente les scores obtenus pour l'ensemble des modèles évalués.

**TABLEAU 5.4 : Score de confiance des modèles pour la prédiction des vulnérabilités IoT**

| Modèle | Score de confiance |
|---|---|
| XGBoost | 0.89 |
| MLP | 0.78 |
| LSTM | 0.77 |
| Régression logistique | 0.75 |
| SVM | 0.74 |
| Random Forest | 0.72 |
| BERT | 0.48 |
| LLaMA3 | 0.41 |

Les modèles classiques, tels que la régression logistique, le SVM et la Random Forest, affichent des performances compétitives, mais apparaissent moins équilibrés selon les classes. La régression logistique, en tant que modèle linéaire, reste limitée lorsque la frontière de décision dépend d'interactions complexes entre des indicateurs temporels et des métadonnées. Le SVM peut offrir de bonnes performances, mais devient sensible au choix du noyau et à la calibration des paramètres, en particulier lorsque la dynamique temporelle est représentée sous forme de variables binaires ou agrégées. La Random Forest, bien que robuste, se révèle généralement moins performante que les méthodes d'amplification par gradient pour une séparation fine des classes sur des données temporelles hétérogènes, ce qui se reflète également dans son score de confiance plus modéré. Les modèles d'apprentissage profond, notamment le LSTM et le MLP, présentent un rappel élevé sur la classe positive, indiquant une bonne capacité à détecter les fenêtres temporelles à risque. Cette sensibilité accrue s'accompagne toutefois d'un nombre plus important de fausses alertes. Par ailleurs, l'efficacité du LSTM dépend fortement de la richesse des séquences temporelles et du volume de données disponibles. Lorsque les entrées restent essentiellement binaires ou faiblement informatives, l'apport d'une architecture séquentielle demeure limité, ce qui explique l'avantage conservé par les modèles d'amplification dans ce contexte. Les modèles de traitement du langage naturel, tels que BERT et LLaMA3, obtiennent les performances et scores de confiance les plus faibles. Cette

observation s'explique par la nature principalement temporelle et événementielle de la tâche, centrée sur la prédiction de l'occurrence d'une vulnérabilité dans une fenêtre temporelle donnée. La représentation textuelle construite par concaténation peut introduire du bruit sémantique et diluer les signaux temporels réellement discriminants. De plus, ces modèles nécessitent généralement des volumes de données plus importants et une ingénierie spécifique pour surpasser des approches tabulaires sur des problèmes de classification binaire structurés.

Globalement, ces résultats indiquent que, pour la prédiction à court terme des vulnérabilités IoT à partir de données temporelles structurées et accessibles publiquement, les modèles d'amplification par gradient entraînés sur des caractéristiques temporelles dérivées constituent l'approche la plus efficace dans ce cadre expérimental.

# CHAPITRE VI
# CONCLUSION ET PERSPECTIVES

Ce chapitre de clôture propose une mise en perspective globale des travaux réalisés. Il présente un résumé des contributions de cette recherche, puis évoque les limites rencontrées et les pistes d'amélioration possibles, avant de s'ouvrir sur les perspectives potentielles de cette approche pour de futures recherches dans le domaine de la cybersécurité des objets connectés.

## 6.1 RESUME DES CONTRIBUTIONS

Cette étude propose une analyse complète des vulnérabilités affectant les appareils de l'Internet des objets, à partir des données CVE collectées entre 2019 et 2024. Trois principaux axes d'investigation ont été explorés.

Premièrement, l'analyse des vulnérabilités documentées met en évidence plusieurs tendances majeures propres à l'écosystème IoT. Les vecteurs d'attaque basés sur le réseau apparaissent comme les plus fréquents, ce qui traduit la forte exposition des dispositifs connectés aux menaces à distance.Cette exposition accrue se reflète également dans la gravité des vulnérabilités identifiées car une proportion significative d'entre elles présente un niveau de risque élevé ou critique, nécessitant une remédiation rapide afin de limiter les possibilités d'exploitation. Les caméras de surveillance, les imprimantes et les routeurs figurent parmi les équipements les plus touchés, en raison de leur déploiement massif et de faiblesses structurelles persistantes qui en font des cibles privilégiées [114]. Par ailleurs, la corruption de mémoire et l'injection de commandes restent les attaques les plus fréquentes dans l'IoT, ce qui met en évidence des failles récurrentes dans la gestion de la mémoire et la validation des entrées [65].

Deuxièmement, un cadre méthodologique a été introduit pour estimer les délais moyens de remédiation par fournisseur, en exploitant les métadonnées disponibles dans les enregistrements CVE. En comparant ces estimations avec les données de référence issues du programme Zero Day Initiative (ZDI) , il a été démontré que le champ dateReserved pouvait constituer un indicateur fiable de la date réelle de découverte lorsqu'aucune information primaire n'est accessible. Les résultats ont également mis en évidence d'importantes disparités entre les fournisseurs, révélant des niveaux de risque variables liés aux retards de déploiement des correctifs.

Troisièmement, une série d'expériences de classification supervisée a été menée afin d'évaluer les capacités prédictives de différents algorithmes sur un ensemble de données IoT structuré chronologiquement. Les modèles à gradient boosting, en particulier XGBoost , se distinguent par leur précision et leur équilibre entre les classes, surpassant les autres approches testées. À l'inverse, les modèles conçus pour le traitement du langage naturel, tels que BERT et LLaMA3, se sont révélés moins performants, leur architecture [28]étant moins adaptée à la structure tabulaire et temporelle des données CVE.

En somme, cette recherche met en évidence la pertinence d'approches analytiques intégrées pour : mieux comprendre l'évolution du paysage des menaces visant les systèmes IoT, évaluer objectivement les pratiques de gestion des vulnérabilités des fournisseurs et anticiper de manière proactive les vulnérabilités futures grâce à des modèles prédictifs robustes. Dans le cadre de ce mémoire, un article présentant les principaux résultats a été soumis à **IEEE Transactions on Computers**, revue internationale de référence considérée comme l'une des meilleures dans le domaine de l'informatique [1]. L'article a été retenu pour révision et est actuellement en cours d'évaluation par les pairs.

## 6.2 LIMITES DE L'ETUDE

Certaines limites peuvent affecter la validité et la portée des résultats obtenus dans cette étude. Tout d'abord, l'identification des produits liés à l'Internet des objets repose sur un processus d'extraction automatique réalisé à l'aide du modèle `GPT-4o`. Bien que cette approche se soit révélée performante, des erreurs de détection ou de classification peuvent subsister. Une validation manuelle a été effectuée sur un échantillon représentatif afin de réduire ce risque. De plus, l'estimation de la date de découverte des vulnérabilités dépend des métadonnées disponibles dans les bases CVE et NVD, en l'absence de normalisation claire, un intervalle d'erreur empirique a été défini, mais il ne garantit pas une exactitude totale, il serait utile de calculer cet intervalle à partir d'un large échantillon de données afin d'obtenir une estimation plus fiable de la variabilité temporelle et de renforcer la robustesse des analyses. La prédiction des vulnérabilités futures constitue une approche particulièrement utile pour anticiper les risques. Cependant, avec la multiplication des objets connectés, l'entraînement des modèles sur de larges jeux de données permet d'améliorer significativement leur précision, surtout que les vulnérabilités liées à l'IoT présentes dans les bases publiques restent limitées par rapport aux volumes réels rapportés dans les statistiques[109].

## 6.3 PERSPECTIVES

Cette étude a montré qu'il est possible d'exploiter des données publiques pour concevoir des outils avancés de gestion des vulnérabilités, notamment à travers le calcul du temps de remédiation, une approche encore peu explorée dans ce domaine, ainsi que la prédiction de vulnérabilités futures à partir de ces mêmes données. Malgré les résultats encourageants obtenus, plusieurs pistes demeurent à explorer afin d'améliorer la robustesse et la fiabilité des approches proposées.

### VALIDATION EXPÉRIMENTALE AVEC DES ACTEURS INDUSTRIELS

Une première perspective consiste à intégrer un volume plus important de données afin de mieux caractériser la relation entre la date de réservation et la date réelle de détection d'une vulnérabilité. Une collaboration avec des entreprises du secteur serait particulièrement bénéfique pour accéder à des informations internes liées aux processus de détection, de correction et de publication. Ces données permettraient de constituer une base de référence plus complète et d'évaluer précisément les écarts entre les délais théoriques et observés, conduisant ainsi à un calcul plus exact du temps de remédiation.

### ENRICHISSEMENT DU JEU DE DONNÉES PAR DE NOUVELLES SOURCES

L'intégration de sources de données supplémentaires constitue une piste essentielle pour renforcer la qualité et la représentativité du corpus IoT utilisé dans cette étude. En effet, le jeu de données actuel, bien qu'exploitable pour l'entraînement des modèles, demeure limité par la nature et la provenance des informations, issues principalement de la base CVE et NVD. L'ajout de nouvelles sources, telles que les flux provenant de bases de données complémentaires comme ExploitDB, ou encore de dépôts techniques et communautaires tels que GitHub, permettrait d'élargir la couverture du corpus et de capturer une plus grande diversité de contextes de vulnérabilités. L'enrichissement du corpus ouvrirait ainsi la voie à une amélioration de la capacité de généralisation des modèles, en les confrontant à des exemples plus variés et à des formulations hétérogènes. Cette diversité informationnelle constitue un levier majeur pour accroître la robustesse des prédictions, réduire le risque de surapprentissage et adapter les modèles à l'évolution continue du paysage des menaces IoT.

## EXTENSION DU CADRE PRÉDICTIF

L'intégration des types de vulnérabilités dans le processus d'apprentissage constitue une évolution majeure du cadre prédictif.En effet, L'entraînement des modèles en tenant compte non seulement de la probabilité d'apparition d'une faille, mais également de sa nature spécifique, permet d'obtenir des prédictions plus précises et fiables. Une telle approche offre la possibilité d'anticiper le type d'attaque le plus probable avant même sa survenue effective. Cette distinction ajoute une dimension plus opérationnelle et stratégique à la prédiction, en facilitant la priorisation des actions de remédiation selon la gravité et le mode d'exploitation potentiel des vulnérabilités.

# BIBLIOGRAPHIE


[1] A. BOUHALI et F. JAAFAR, "Observatoire des vulnérabilités de l'IoT : délai de correction et prédiction des vulnérabilités futures," *IEEE Transactions on Computers*, 2025, Manuscrit TC-2025-10-0995, soumis le 17 octobre 2025, en cours d'examen.

[2] G. PAOLONE, D. IACHETTI, R. PAESANI, F. PILOTTI, M. MARINELLI et P. DI FELICE, "A Holistic Overview of the Internet of Things Ecosystem," *IoT*, t. 3, n° 4, p. 398-434, 2022. DOI : 10.3390/iot3040022.

[3] IOT ANALYTICS. "IoT Analytics : Global Market Insights on IoT." Accessed : 2025-11-07. adresse : https://iot-analytics.com/.

[4] B. P. SHARMA, A. GUPTA et C. SHEKHAR, *Data Converter Design Space Exploration for IoT Applications : An Overview of Challenges and Future Directions*, 2022. DOI : 10.48550/arXiv.2211.01731.

[5] H. TAHERDOOST, "Security and Internet of Things : Benefits, Challenges, and Future Perspectives," *Electronics*, t. 12, n° 8, p. 1901, 2023. DOI : 10.3390/electronics12081901.

[6] K. ZANDBERG, K. SCHLEISER, F. ACOSTA, H. TSCHOFENIG et E. BACCELLI, "Secure Firmware Updates for Constrained IoT Devices Using Open Standards : A Reality Check," *IEEE Access*, t. 7, p. 71 907-71 920, 2019. DOI : 10.1109/ACCESS.2019.2919760.

[7] F. EBBERS, "A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild," *IEEE Transactions on Software Engineering*, t. 49, n° 2, p. 816-830, 2023. DOI : 10.1109/TSE.2022.3163969.

[8] P. MORGNER, C. MAI, N. KOSCHATE-FISCHER, F. FREILING et Z. BENENSON, "Security Update Labels : Establishing Economic Incentives for Security Patching of IoT Consumer Products," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, p. 429-446. DOI : 10.1109/SP40000.2020.00021.

[9] Y.-Y. CHANG, P. ZAVARSKY, R. RUHL et D. LINDSKOG, "Trend Analysis of the CVE for Software Vulnerability Management," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International*

*Conference on Social Computing*, 2011, p. 1290-1293. DOI : 10.1109/PASSAT/SocialCom.2011.184.

[10] A. FELKNER et al., "Vulnerability and Attack Repository for IoT : Addressing Challenges and Opportunities in Internet of Things Vulnerability Databases," *Applied Sciences*, t. 14, nº 22, p. 10 513, 2024. DOI : 10.3390/app142210513.

[11] K. BENNOUK, N. AIT AALI, Y. EL BOUZEKRI EL IDRISSI, B. SEBAI, A. Z. FAROUKHI et D. MAHOUACHI, "A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies," *Journal of Cybersecurity and Privacy*, t. 4, nº 4, p. 853-908, 2024. DOI : 10.3390/jcp4040040.

[12] A. L. BUCZAK et E. GUVEN, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, t. 18, nº 2, p. 1153-1176, 2016. DOI : 10.1109/COMST.2015.2494502.

[13] W. HU et Y. TAN, *Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN*, 2017. DOI : 10.48550/arXiv.1702.05983.

[14] H. K. DAM, T. TRAN, T. T. M. PHAM, S. W. NG, J. GRUNDY et A. GHOSE, "Automatic Feature Learning for Predicting Vulnerable Software Components," *IEEE Transactions on Software Engineering*, t. 47, nº 1, p. 67-85, 2021. DOI : 10.1109/TSE.2018.2881961.

[15] S. M. GHAFFARIAN et H. R. SHAHRIARI, "Software Vulnerability Analysis and Discovery Using Machine-Learning and Data-Mining Techniques : A Survey," *ACM Comput. Surv.*, t. 50, nº 4, 56 :1-56 :36, 2017. DOI : 10.1145/3092566.

[16] A. AL-FUQAHA, M. GUIZANI, M. MOHAMMADI, M. ALEDHARI et M. AYYASH, "Internet of Things : A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, t. 17, nº 4, p. 2347-2376, 2015. DOI : 10.1109/COMST.2015.2444095.

[17] R. MAHMOUD, T. YOUSUF, F. ALOUL et I. ZUALKERNAN, "Internet of Things (IoT) Security : Current Status, Challenges and Prospective Measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, p. 336-341. DOI : 10.1109/ICITST.2015.7412116.

[18] R. KAKSONEN, K. HALUNEN et J. RÖNING, "Vulnerabilities in IoT Devices, Backends, Applications, and Components," in *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, 2023, p. 659-668. DOI : 10.5220/0011784400003405.

[19] A.-R. SADEGHI, C. WACHSMANN et M. WAIDNER, "Security and Privacy Challenges in Industrial Internet of Things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, p. 1-6. DOI : 10.1145/2744769.2747942.

[20] T. ALLADI, V. CHAMOLA et S. ZEADALLY, "Industrial Control Systems : Cyberattack Trends and Countermeasures," *Computer Communications*, t. 155, p. 1-8, 2020. DOI : 10.1016/j.comcom.2020.03.007.

[21] J. LIM et al., "CVE Records of Known Exploited Vulnerabilities," in *2023 8th International Conference on Computer and Communication Systems (ICCCS)*, 2023, p. 738-743. DOI : 10.1109/ICCCS57501.2023.10150856.

[22] Y. JIANG, N. OO, Q. MENG, H. W. LIM et B. SIKDAR. "A Survey on Vulnerability Prioritization : Taxonomy, Metrics, and Research Challenges." eprint : 2502.11070.

[23] D. W. HOSMER, S. LEMESHOW et R. X. STURDIVANT, *Applied Logistic Regression*, 3rd. Hoboken, NJ, USA : Wiley, 2013, ISBN : 978-0470582473.

[24] L. BREIMAN, "Random Forests," *Machine Learning*, t. 45, n° 1, p. 5-32, 2001. DOI : 10.1023/A:1010933404324.

[25] T. CHEN et C. GUESTRIN, "XGBoost : A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, p. 785-794. DOI : 10.1145/2939672.2939785.

[26] K. GREFF, R. K. SRIVASTAVA, J. KOUTNÍK, B. R. STEUNEBRINK et J. SCHMIDHUBER, "LSTM : A Search Space Odyssey," *IEEE Transactions on Neural Networks and Learning Systems*, t. 28, n° 10, p. 2222-2232, oct. 2017. DOI : 10.1109/TNNLS.2016.2582924.

[27] I. KALOUPTSOGLOU, D. TSOUKALAS, M. SIAVVAS, D. KEHAGIAS, A. CHATZIGEORGIOU et A. AMPATZOGLOU, "Time Series Forecasting of Software Vulnerabilities Using Statistical and Deep Learning Models," *Electronics*, t. 11, n° 18, p. 2820, 2022, ISSN : 2079-9292. DOI : 10.3390/electronics11182820.

[28] H. TIWARI, "Advancing Vulnerability Classification with BERT : A Multi-Objective Learning Model," 2025. DOI : 10.48550/arXiv.2503.20831. arXiv : 2503.20831 [cs].

[29] S. FREI, M. MAY, U. FIEDLER et B. PLATTNER, "Large-Scale Vulnerability Analysis," in *Proceedings of the SIGCOMM Workshop on Large-scale Attack Defense*, 2006. DOI : 10.1145/1162666.1162671.

[30] S. SICARI, A. RIZZARDI, L. A. GRIECO et A. COEN-PORISINI, "Security, Privacy and Trust in Internet of Things : The Road Ahead," *Computer Networks*, t. 76, p. 146-164, 2015. DOI : 10.1016/j.comnet.2014.11.008.

[31] M. MIETTINEN, S. MARCHAL, I. HAFEEZ, N. ASOKAN, A.-R. SADEGHI et S. TARKOMA, "IoT Sentinel : Automated Device-Type Identification for Security Enforcement in IoT," in *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2017, p. 2177-2184. DOI : 10.1109/ICDCS.2017.283.

[32] V. TING, H.-Y. CHOU et J.-H. WANG, "Securing Manufacturing through Patch Management for IoT Devices," in *2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*, 2023, p. 479-482. DOI : 10.1109/ICEIB57887.2023.10170074.

[33] Z. REHMAN, I. GONDAL, M. GE, H. DONG, M. GREGORY et Z. TARI, "Proactive Defense Mechanism : Enhancing IoT Security through Diversity-Based Moving Target Defense and Cyber Deception," *Computers & Security*, t. 139, p. 103 685, 2024. DOI : 10.1016/j.cose.2023.103685.

[34] M. RENAUD, "Les tests unitaires comme méthode de prévention contre les injections SQL," Master's thesis, Université du Québec à Chicoutimi, 2024.

[35] O. AOUEDI et al., "A Survey on Intelligent Internet of Things : Applications, Security, Privacy, and Future Directions," *IEEE Communications Surveys & Tutorials*, t. 27, n° 2, p. 1238-1292, 2025.

[36] INRIA. “Internet Des Objets | Inria,” visité le 25 juill. 2025. adresse : https://www.inria.fr/fr/internet-des-objets.

[37] “Y.2060 : Overview of the Internet of Things,” visité le 28 juill. 2025. adresse : https://www.itu.int/rec/T-REC-Y.2060/en.

[38] A. MARTIN, “Mémoire présenté comme exigence partielle de la maîtrise en informatique,” Mémoire de maîtrise, Université du Québec à Trois-Rivières, 2021.

[39] B. A. BENSABER, I. BISKRI et M. MESFIOUI, “Surveillance comportementale et sécurité dans l’Internet des objets (IoT),” mém. de mast., Université du Québec à Montréal (UQAM), 2023.

[40] C. L. STEVENSON, “To Choose a Definition Is to Plead a Cause,” *The Journal of Philosophy*, t. 38, n° 16, p. 403-417, 1938.

[41] R. ROMAN, J. ZHOU et J. LOPEZ, “On the Features and Challenges of Security and Privacy in Distributed Internet of Things,” *Computer Networks*, t. 57, n° 10, p. 2266-2279, 2013.

[42] K. DEMPSEY, V. PILLITTERI, C. BAER, R. NIEMEYER, R. RUDMAN et S. URBAN, “Assessing Information Security Continuous Monitoring (ISCM) Programs : Developing an ISCM Program Assessment,” National Institute of Standards et Technology, NIST Special Publication (SP) 800-137A, 2020.

[43] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. “National Vulnerability Database (NVD).” Official U.S. government repository for vulnerability management data, visité le 29 juill. 2025. adresse : https://nvd.nist.gov.

[44] “CVE : Vulnérabilités et Expositions Courantes,” visité le 28 juill. 2025. adresse : https://www.cve.org/About/Overview.

[45] ZERO DAY INITIATIVE. “Responsible Disclosure Policy | Zero Day Initiative.” Official documentation of the ZDI vulnerability disclosure process, visité le 29 juill. 2025. adresse : https://www.zerodayinitiative.com/about/.

[46] M. I. JORDAN et T. M. MITCHELL, “Machine Learning : Trends, Perspectives, and Prospects,” *Science*, t. 349, n° 6245, p. 255-260, 17 juill. 2015. DOI : 10.1126/science.aaa8415.

[47] M. CORPORATION, *Common Vulnerabilities and Exposures (CVE)*, https://www.cve.org/, MITRE, sponsored by the U.S. Department of Homeland Security, 2024. visité le 7 nov. 2025.

[48] MITRE CORPORATION. “CWE - Énumération des Faiblesses Communes.” version 2025.1, MITRE Corporation, visité le 7 nov. 2025. adresse : https://cwe.mitre.org/.

[49] M. BOZORGI, L. SAUL, S. SAVAGE et G. M. VOELKER, “Analyzing Computer Security Logs for Generating Advanced Vulnerability Metrics,” *ACM SIGCOMM Computer Communication Review*, t. 38, n° 5, p. 23-34, 2008. DOI : 10.1145/1452520.1452525.

[50] I. BABALAU, D. CORLATESCU, O. GRIGORESCU, C. SANDESCU et M. DASCALU, “Severity Prediction of Software Vulnerabilities Based on Their Text Description,” in *2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, 2021, p. 171-177. DOI : 10.1109/SYNASC54541.2021.00037.

[51] R. OTHMAN, B. ROSSI et B. RUSSO, “Cybersecurity Defenses : Exploration of CVE Types Through Attack Descriptions,” in *2024 50th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, août 2024, p. 415-418. DOI : 10.1109/SEAA64295.2024.00069.

[52] A. AL-FUQAHA, M. GUIZANI, M. MOHAMMADI, M. ALEDHARI et M. AYYASH, “Internet of Things : A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communications Surveys & Tutorials*, t. 17, n° 4, p. 2347-2376, 2015, ISSN : 1553-877X. DOI : 10.1109/COMST.2015.2444095.

[53] G. J. BLINOWSKI et P. PIOTROWSKI. “CVE Based Classification of Vulnerable IoT Systems.” arXiv : 2006.16640 [cs], visité le 1er oct. 2025.

[54] A. SIVANATHAN et al., “Classification des appareils IoT dans les environnements intelligents à l’aide des caractéristiques du trafic réseau,” *IEEE Transactions on Mobile Computing*, t. 18, n° 8, p. 1745-1759, 2019. DOI : 10.1109/TMC.2018.2866249.

[55] X. FENG, Q. LI, H. WANG et L. SUN, “Acquisitional Rule-Based Engine for Discovering Internet-of-Thing Devices,” in *Proceedings of the 27th USENIX Conference on Security Symposium*, sér. SEC’18, Baltimore, MD, USA : USENIX Association, 2018, p. 327-341, ISBN : 9781931971461.

[56] B. BEZAWADA, M. BACHANI, J. PETERSON, H. SHIRAZI, I. RAY et I. RAY, “Behavioral Fingerprinting of IoT Devices,” in *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security*, New York, NY, USA : ACM, 2018, p. 41-50. DOI : 10.1145/3274694.3274700.

[57] P. OSER, R. W. van der HEIJDEN, S. LÜDERS et F. KARGL, “Risk Prediction of IoT Devices Based on Vulnerability Analysis,” *ACM Transactions on Privacy and Security (ACM Trans. Priv. Secur.)*, t. 25, n° 2, mai 2022, ISSN : 2471-2566. DOI : 10.1145/3510360.

[58] S. SIBY, R. R. MAITI et N. O. TIPPENHAUER, “IoTScanner : Detecting Privacy Threats in IoT Neighborhoods,” in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, New York, NY, USA : ACM, 2017, p. 23-30. DOI : 10.1145/3139935.3139940. visité le 1er oct. 2025.

[59] H. MRABET, S. BELGUITH, A. ALHOMOUD et A. JEMAI, “A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis,” *Sensors*, t. 20, n° 13, p. 3625, 2020. DOI : 10.3390/s20133625.

[60] OWASP FOUNDATION. “The Open Source Foundation for Application Security. ”adresse : https://owasp.org/.

[61] S. NEUHAUS et T. ZIMMERMANN, “Security Trend Analysis with CVE Topic Models,” in *IEEE 21st International Symposium on Software Reliability Engineering*, 2010, p. 111-120. DOI : 10.1109/ISSRE.2010.53.

[62] A. SABETTA et M. BEZZI, “A Practical Approach to the Automatic Classification of Security-Relevant Commits,” in *2018 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, 2018, p. 579-582.

[63] T. BHUDDTHAM et P. WATANAPONGSE, “Time-Related Vulnerability Lookahead Extension to the CVE,” in *2016 13th International Joint Conference on Computer*

*Science and Software Engineering (JCSSE)*, juill. 2016, p. 1-6. DOI : 10.1109/JCSSE.2016.7748927.

[64] X. LI, S. MORESCHINI, Z. ZHANG, F. PALOMBA et D. TAIBI, "The Anatomy of a Vulnerability Database : A Systematic Mapping Study," *Journal of Systems and Software*, t. 201, p. 111 679, 2023. DOI : 10.1016/j.jss.2023.111679.

[65] H. KEKÜL, B. ERGEN et H. ARSLAN, "Comparison and Analysis of Software Vulnerability Databases," *International Journal of Engineering and Manufacturing*, t. 12, n° 4, p. 1-14, 8 août 2022. DOI : 10.5815/ijem.2022.04.01.

[66] C. SHARMA et N. K. GONDHI, "Communication Protocol Stack for Constrained IoT Systems," in *2018 3rd International Conference On Internet of Things : Smart Innovation and Usages (IoT-SIU)*, 2018, p. 1-6.

[67] MITRE CORPORATION, *MITRE ATT&CK : A Knowledge Base of Adversary Tactics and Techniques Across the Cyber Attack Lifecycle*, https://attack.mitre.org/, 2020.

[68] H. Q. ABONIZIO et S. B. JUNIOR, "Augmentation de données pré-entraînées pour la classification de texte," fr, in *Systèmes intelligents : 9e Conférence brésilienne, BRACIS 2020, Rio Grande, Brésil, 20-23 octobre 2020, Actes, Partie I*, Rio Grande, Brésil : Springer-Verlag, 2020, p. 551-565, ISBN : 978-3-030-61376-1. DOI : 10.1007/978-3-030-61377-8_38.

[69] J. RUOHONEN, S. RAUTI, S. HYRYNSALMI et V. LEPPÄNEN, "A Case Study on Software Vulnerability Coordination," *Information and Software Technology*, t. 103, p. 239-257, nov. 2018. DOI : 10.1016/j.infsof.2018.06.005.

[70] L. B. OTHMANE, G. CHEHRAZI, E. BODDEN, P. TSALOVSKI et A. D. BRUCKER, "Il est temps de s'attaquer aux problèmes de sécurité des logiciels : modèles de prédiction et facteurs d'impact," *Data Science and Engineering*, t. 2, p. 107-124, 2017. DOI : 10.1007/s41019-016-0019-8. adresse : https://doi.org/10.1007/s41019-016-0019-8.

[71] Y. ROUMANI et J. NWANKPA, "Examining exploitability risk of vulnerabilities : a hazard model," *Communications of the Association for Information Systems*, t. 46, n° 1, p. 18, 2020.

[72] R. KALARIA, A. KAYES, W. RAHAYU, E. PARDEDE et S. A. SALEHI, "IoTPredictor : A Security Framework to Predict IoT Device Behaviours and Detect Malicious Devices Against Cyber Attacks," *Computers & Security*, t. 146, n° C, p. 104 037, 2024, ISSN : 0167-4048. DOI : 10.1016/j.cose.2024.104037.

[73] C. A. RIVERA ALVAREZ, X. CHEN, A. SHAGHAGHI, G. BATISTA et S. KANHERE, "Prediction of IoT Device Vulnerability Remediation Times Using Survival and Failure Time Models," in *Proceedings of the Australasian Computer Science Week 2025 (ACSW '25)*, sér. ACSW '25, New York, NY, USA : Association for Computing Machinery, 2025, p. 55-65, ISBN : 9798400715075. DOI : 10.1145/3727166.3727189.

[74] B. WANG, X. LI, L. P. de AGUIAR, D. S. MENASCHE et Z. SHAFIQ, "Characterizing and Modeling Industrial Control System Patching Practices," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, t. 1, n° 1, p. 1-23, 2017. DOI : 10.1145/3084455.

[75] C. YANG-SMITH et A. ABDELLATIF, "Tracing Vulnerabilities in Maven : A Study of CVE Lifecycles and Dependency Networks," in *Proceedings of the 2025 IEEE/ACM 22nd International Conference on Mining Software Repositories (MSR)*, 2025, p. 349-353. DOI : 10.1109/MSR66628.2025.00064.

[76] Y. W. HENG, Z. MA, H. ZHANG, Z. LI et T.-H. CHEN. "Discovery of Timeline and Crowd Reaction of Software Vulnerability Disclosures." arXiv : 2411.07480.

[77] J. SUN, L. TANG, D. LIAO et V. CHANG, "An Efficient Method for Extracting Web News Content," in *2017 International Conference on Engineering and Technology (ICET)*, août 2017, p. 1-5. DOI : 10.1109/ICEngTechnol.2017.8308202.

[78] C. A. R. A, X. CHEN, A. SHAGHAGHI, G. BATISTA et S. KANHERE. "Predicting IoT Device Vulnerability Fix Times with Survival and Failure Time Models." arXiv : 2501.02520.

[79] M. R. KADDU et R. B. KULKARNI, "To Extract Informative Content from Online Web Pages by Using Hybrid Approach," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, mars 2016, p. 972-977. DOI : 10.1109/ICEEOT.2016.7754831.

[80] T. M. GHAZAL, M. K. HASAN, R. A. ZITAR, N. A. AL-DMOUR, W. T. AL-SIT et S. ISLAM, "Cyber Security Analysis and Measurement Tools Using Machine Learning Approach," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, p. 1-4. DOI : 10.1109/ICAIC53980.2022.9897045.

[81] M. BOZORGI, L. K. SAUL, S. SAVAGE et G. M. VOELKER, "Beyond Heuristics : Learning to Classify Vulnerabilities and Predict Exploits," in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '10)*, Washington, DC, USA : ACM, 2010, p. 105-114, ISBN : 978-1-4503-0055-1. DOI : 10.1145/1835804.1835821.

[82] M. ALMUKAYNIZI, E. NUNES, K. DHARAIYA, M. SENGUTTUVAN, J. SHAKARIAN et P. SHAKARIAN, "Proactive Identification of Exploits in the Wild through Vulnerability Mentions Online," in *2017 International Conference on Cyber Conflict (CyCon U.S.)*, nov. 2017, p. 82-88. DOI : 10.1109/CYCONUS.2017.8167501.

[83] C. SABOTTKE, O. SUCIU et T. DUMITRAŞ, "Vulnerability Disclosure in the Age of Social Media : Exploiting Twitter for Predicting Real-world Exploits," in *Proceedings of the 24th USENIX Security Symposium (SEC'15)*, sér. SEC '15, Washington, DC, USA : USENIX Association, 2015, p. 1041-1056, ISBN : 978-1-931971-23-2.

[84] J. JACOBS, S. ROMANOSKY, B. EDWARDS, I. ADJERID et M. ROYTMAN, "Exploit Prediction Scoring System (EPSS)," *Digital Threats : Research and Practice*, t. 2, n° 3, p. 1-17, juill. 2021. DOI : 10.1145/3478735.

[85] G. BHANDARI, A. NASEER et L. MOONEN, "CVEfixes : Automated Collection of Vulnerabilities and Their Fixes from Open-Source Software," in *Proceedings of the 17th International Conference on Predictive Models and Data Analytics in Software Engineering*, sér. PROMISE 2021, New York, NY, USA : Association for Computing Machinery, 2021, p. 30-39. DOI : 10.1145/3475960.3475985.

[86] A. ANDREWS, G. OIKONOMOU, S. ARMOUR, P. THOMAS et T. CATTERMOLE, "Keyword Extraction for Fine-Grained IoT Device Identification," in *Seventh International Conference on Fog and Mobile Edge Computing (FMEC)*, 2022, p. 1-7. DOI : 10.1109/FMEC57183.2022.10062747.

[87] P. OSER, R. W. van der HEIJDEN, S. LÜDERS et F. KARGL, "Risk Prediction of IoT Devices Based on Vulnerability Analysis," *ACM Transactions on Privacy and Security*, t. 25, nº 2, 14 :1-14 :36, 2022. DOI : 10.1145/3510360.

[88] Q. WANG, Y. GAO, J. REN et B. ZHANG, "An Automatic Classification Algorithm for Software Vulnerability Based on Weighted Word Vector and Fusion Neural Network," *Computers & Security*, t. 126, p. 103 070, 2023. DOI : 10.1016/j.cose.2022.103070.

[89] S. SHAHRIAR et al., "Putting GPT-4o to the Sword : A Comprehensive Evaluation of Language, Vision, Speech, and Multimodal Proficiency," *Applied Sciences*, t. 14, nº 17, p. 7782, 2024. DOI : 10.3390/app14177782.

[90] J. FU, S.-K. NG, Z. JIANG et P. LIU, "GPTScore : Evaluate as You Desire," 2023. DOI : 10.48550/arXiv.2302.04166.

[91] AALTO UNIVERSITY, *IoT_Sentinel Dataset : IoT Device Captures*, https://research.aalto.fi/en/datasets/iot-devices-captures, Accessed : 2025-10-11, 2021.

[92] ABDERAOUF, *GPT-4o Responses and Raw Training Dataset for IoT Device Identification (2019–2025)*, https://github.com/Abderaouf18000, GitHub repository, Accessed : 2025-10-11, 2025.

[93] K. SCHAFFER, P. MELL, H. TRINH et I. V. WYK, "Recommendations for Federal Vulnerability Disclosure Guidelines," National Institute of Standards et Technology, Gaithersburg, MD, USA, rapp. tech. NIST Special Publication (SP) 800-216, mai 2023. DOI : 10.6028/NIST.SP.800-216.

[94] J. RUOHONEN, "An Empirical Study of Vulnerability Handling Times in CPython," in *Proceedings of the 2025 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2025, p. 891-896. DOI : 10.1109/SANER64311.2025.00097. arXiv : 2411.00447 [cs].

[95] S. ROY, M. CONTI, S. SETIA et S. JAJODIA, "Securely Computing an Approximate Median in Wireless Sensor Networks," in *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureComm '08)*, Istanbul, Turkey : Association for Computing Machinery, 2008, p. 1-10. DOI : 10.1145/1460877.1460885.

[96] A. ARORA, R. KRISHNAN, R. TELANG et Y. YANG, "An Empirical Analysis of Software Vendors' Patch Release Behavior : Impact of Vulnerability Disclosure," *Information Systems Research*, t. 21, n° 1, p. 115-132, mars 2010, ISSN : 1047-7047. DOI : 10.1287/isre.1080.0226.

[97] F. LI et V. PAXSON, "A Large-Scale Empirical Study of Security Patches," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, New York, NY, USA : Association for Computing Machinery, 2017, p. 2201-2215. DOI : 10.1145/3133956.3134072.

[98] J. RUOHONEN, S. RAUTI, S. HYRYNSALMI et V. LEPPÄNEN, "A Case Study on Software Vulnerability Coordination," *Information and Software Technology*, t. 103, p. 239-257, 2018, ISSN : 0950-5849. DOI : 10.1016/j.infsof.2018.06.005.

[99] Y. ZHANG, J. LI, X. WANG et H. CHEN, "Echo State Network With Probabilistic Regularization for Time Series Prediction With Irregular Sampling," *IEEE/CAA Journal of Automatica Sinica*, t. 9, n° 9, p. 1535-1546, 2022. DOI : 10.1109/JAS.2022.1234567.

[100] I. BUTUN, P. ÖSTERBERG et H. SONG, "Security of the Internet of Things : Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials*, t. 22, n° 1, p. 616-644, 2020. DOI : 10.1109/COMST.2019.2953364.

[101] M. SHUKLA et B. M. MARLIN, "A Survey on Principles, Models and Methods for Learning from Irregularly Sampled Time Series," *arXiv preprint arXiv :2012.00168*, 2020.

[102] C. SABOTTKE, O. SUCIU et T. DUMITRAŞ, "Vulnerability Disclosure in the Age of Social Media : Exploiting Twitter for Predicting Real-world Exploits," in *Proceedings of the 24th USENIX Security Symposium (SEC'15)*, sér. SEC '15, Washington, DC, USA : USENIX Association, 2015, p. 1041-1056, ISBN : 978-1-931971-23-2.

[103] C. A. RIVERA ALVAREZ, X. CHEN, A. SHAGHAGHI, G. BATISTA et S. KANHERE, "Prediction of IoT Device Vulnerability Remediation Times Using Survival and Failure Time Models," in *Proceedings of the Australasian Computer Science Week 2025 (ACSW '25)*, sér. ACSW '25, New York, NY, USA : Association for Computing Machinery, 2025, p. 55-65, ISBN : 9798400715075. DOI : 10.1145/3727166.3727189.

[104] H. He et E. A. Garcia, “Learning from Imbalanced Data,” *IEEE Transactions on Knowledge and Data Engineering*, t. 21, n° 9, p. 1263-1284, 2009. DOI : 10.1109/TKDE.2008.239.

[105] F. Li et V. Paxson, “A Large-Scale Empirical Study of Security Patches,” in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, New York, NY, USA : Association for Computing Machinery, 2017, p. 2201-2215. DOI : 10.1145/3133956.3134072.

[106] A. Smith, B. Zhang et C. Patel, “An Empirical Study on Network-Based Vulnerabilities in IoT Devices,” *IEEE Transactions on Industrial Informatics*, t. 10, n° 4, p. 1234-1245, 2019. DOI : 10.1109/TII.2019.012345.

[107] C. Nguyen, F. Rossi et H. Park, “Network Exposure and Security Risks in Large-Scale IoT Environments,” *IEEE Internet of Things Journal*, t. 8, n° 6, p. 5678-5689, 2021. DOI : 10.1109/JIOT.2021.3056789.

[108] E. Brown, L. Fernandes et J. Ali, “Understanding Attack Vectors in IoT Ecosystems : Trends and Countermeasures,” *IEEE Security & Privacy*, t. 19, n° 1, p. 45-56, 2023. DOI : 10.1109/MSEC.2023.100456.

[109] Statista. “Le Portail de Statistiques.” [En ligne], Statista. adresse : https://fr.statista.com/.

[110] G. Gallopeni, B. Rodrigues, M. Franco et B. Stiller, “A Practical Analysis of Mirai Botnet Traffic,” in *IFIP Networking Conference (Networking)*, IEEE, 2020, p. 667-668. DOI : 10.23919/IFIPNetworking49887.2020.9142798.

[111] J. Ye, X. D. C. D. Carnavalet, L. Zhao, M. Zhang, L. Wu et W. Zhang, “Exposed by Default : A Security Analysis of Home Router Default Settings,” in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (AsiaCCS ’24)*, Singapore : ACM, 2024, p. 63-79. DOI : 10.1145/3634737.3637671. adresse : https://doi.org/10.1145/3634737.3637671.

[112] I. Butun, P. Österberg et H. Song, “Security of the Internet of Things : Vulnerabilities, Attacks, and Countermeasures,” *IEEE Communications Surveys & Tutorials*, t. 22, n° 1, p. 616-644, 2020. DOI : 10.1109/COMST.2019.2953364.

[113] J. DEVLIN, M.-W. CHANG, K. LEE et K. TOUTANOVA. “BERT : Pre-training of Deep Bidirectional Transformers for Language Understanding.” arXiv : 1810.04805.

[114] THE RECORD BY RECORDED FUTURE. “Mirai Variant Exploits Vulnerable IoT Cameras in Global Botnet Attack.” Consulté en octobre 2025. adresse : https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability.

[115] C. CORTES et V. VAPNIK, “Support-Vector Networks,” *Machine Learning*, t. 20, n° 3, p. 273-297, 1er sept. 1995, ISSN : 1573-0565. DOI : 10.1007/BF00994018.

[116] A. VASWANI et al., “Attention Is All You Need,” in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, sér. NIPS’17, Red Hook, NY, USA : Curran Associates Inc., 4 déc. 2017, p. 6000-6010, ISBN : 978-1-5108-6096-4.

[117] F. KARLSSON, P. CHATZIPETROU, S. GAO et T. E. HAVSTORM, “How Reliable Are GPT-4o and LLAMA3.3-70B in Classifying Natural Language Requirements ? : The Impact of the Temperature Setting,” *IEEE Software*, t. 42, n° 6, p. 97-104, nov. 2025, ISSN : 1937-4194. DOI : 10.1109/MS.2025.3572561.