Apprentissage automatique pour la détection des attaques DoS dans les systèmes IoT

Mémoire présenté

dans le cadre du programme de maîtrise en informatique

en vue de l'obtention du grade maître ès sciences (M.Sc.)

PAR

© Brunel Rolack KIKISSAGBE

Novembre 2024

Composition du jury :

Barka Noureddine, président du jury, UQAR

Meddi Adda, directeur de recherche, UQAR

Martin Otis, examinateur externe, UQAC

Eugene EZIN, examinateur externe, UAC Benin

Dépôt initial le 24 Aout 2024 Dépôt final le 14 Novembre 2024

REMERCIEMENTS

Je tiens tout d'abord à exprimer ma profonde gratitude envers mon directeur de recherche, Mehdi Adda, pour sa présence constante, son attention et ses précieux conseils tout au long de ce travail de recherche. Je le remercie également pour sa gentillesse, sa patience, le temps inconditionnel qu'il m'a consacré et ses précieuses observations qui m'ont beaucoup appris sur la conduite de ce travail de recherche

Je souhaite également adresser mes remerciements les plus sincères à mes parents, Mohamed ADJADI et Alake AFFOGNON, pour leur soutien indéfectible malgré la distance qui nous sépare. A ma sœur, Oslyne KIKISSAGBE, je suis reconnaissant pour son soutien précieux et son encouragement tout au long de cette aventure académique malgré la distance qui nous sépare.

Enfin, un grand merci à tous mes amis particulièrement Wallys et Arsène, pour leur présence et leur soutien constant. Votre amitié m'a été d'un grand réconfort. Je vous suis infiniment reconnaissant à tous pour avoir enrichi cette expérience par votre soutien et votre présence à mes côtés. Je souhaite également exprimer ma gratitude envers Kamilath pour son soutien précieux tout au long de ce parcours

RÉSUMÉ

Dans le domaine en constante évolution des technologies de l'information, l'Internet des Objets (IdO) a émergé comme une innovation révolutionnaire, intégrant des objets du quotidien à l'Internet, ce qui rend notre environnement plus interactif et automatisé. Cette expansion rapide de l'IdO pose des problèmes en matière de sécurité au niveau des appareils IdO. Les attaques par déni de service (DoS) sont particulièrement alarmantes, car elles peuvent perturber ou paralyser les réseaux. Il est donc important de mettre en place un mécanisme robuste permettant de prévenir ces attaques afin de garantir la disponibilité des services dans l'IoT.

Face à ces défis, les systèmes de Détection d'Intrusion (IDS) sont devenus des outils essentiels pour protéger les infrastructures IoT contre les attaques malveillantes. Cependant, les méthodes traditionnelles de détection d'intrusions ne sont souvent pas adaptées aux spécificités de l'IoT, telles que la diversité des appareils et des protocoles, ainsi que les contraintes de traitement et de stockage.

Ce mémoire présente une étude approfondie sur la détection des attaques par Déni de Service (DoS) dans les systèmes IoT en utilisant l'apprentissage automatique. En combinant des techniques avancées d'équilibrage de classes telles que le suréchantillonnage des minorités synthétiques (SMOTE) et le sous-échantillonnage aléatoire (Random Undersampling), avec des techniques de sélection de fonctionnalités telles que les réseaux de neurones profonds (DNN), Random Forest (RF) et l'analyse en composantes principales (PCA), ainsi que des classificateurs tels que le Support Vector Machine (SVM), XGBoost et le DNN, ces modèles visent à améliorer la précision et l'efficacité de la détection des attaques DoS.

Les différentes combinaisons conduisent à des résultats prometteurs dans la classification des attaques DoS dans les systèmes IoT. Les expériences ont montré que l'intégration de diverses techniques de sélection de caractéristiques, d'équilibrage de classes et de classification peut améliorer significativement la détection des attaques. Parmi ces combinaisons, la combinaison du DNN pour la sélection des caractéristiques, du suréchantillonnage SMOTE pour l'équilibrage des classes et du classificateur DNN a démontré une performance exceptionnelle. Cette approche a atteint un taux de précision de 0.9962, une précision de 0.9828, un rappel de 0.9913 et un score F1 de 0.9559, indiquant une capacité remarquable à détecter efficacement les attaques DoS tout en maintenant un faible taux de faux positifs.L'étude souligne aussi l'importance de l'équilibrage des classes et de la sélection des caractéristiques dans le processus de détection des attaques. En combinant ces deux techniques, il a été possible d'améliorer significativement les performances du modèle par rapport aux approches traditionnelles.

Mots clés : IdO ; Sécurité ; Detection d’Intrusion ; Apprentissage automatique ; DoS

ABSTRACT

In the ever-evolving field of information technology, the Internet of Things (IoT) has emerged as a revolutionary innovation, integrating everyday objects with the Internet, making our environment more interactive and automated. This rapid expansion of the IoT poses security challenges for IoT devices. DoS and DDoS attacks are particularly alarming, as they can disrupt or paralyze networks. It is therefore important to put in place a robust mechanism to prevent such attacks, in order to guarantee the availability of services in the IoT.

Faced with these challenges, IDS have become essential tools for protecting IoT infrastructures against malicious attacks. However, traditional intrusion detection methods are often not adapted to the specificities of the IoT, such as the diversity of devices and protocols, as well as processing and storage constraints.

This dissertation presents an in-depth study on the development of a learning model for the detection of DoS attacks in IoT systems. By combining advanced class balancing techniques such as SMOTE and Random Undersampling , with feature selection techniques such as DNN, Random Forest and PCA, as well as classifiers such as SVM, XGBoost and DNN, this model aims to improve the accuracy and efficiency of DoS attack detection.

The different combinations lead to promising results in classifying DoS attacks in IoT systems. The experiments showed that integrating various feature selection, class balancing, and classification techniques can significantly improve attack detection. Among these combinations, the use of DNN for feature selection, SMOTE oversampling for class balancing, and the DNN classifier demonstrated exceptional performance. This approach achieved an accuracy of 0.9962, a precision of 0.9828, a recall of 0.9913, and an F1 score of 0.9559, highlighting a remarkable capacity to effectively detect DoS attacks while maintaining a low false positive rate. The study also highlights the importance of class balancing and feature selection in the attack detection process. By combining these two techniques, it was possible to significantly improve model performance over traditional approaches.

Keywords: IoT; Security ; Intrusion Detection ; Machine Learning ; DoS

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

AI	Artificielle Intelligence
ML	Machine Learning
IoT	Internet of Things
IdO	Internet des Objets
IDS	Intrusion Detection System
DL	Deep Learning
RNN	Recurrent Neural Network
ANN	Artificial Neural Network
CNN	Convolutional Neural Network
DNN	Deep Neural Network
KNN	K-Nearest Neighbors
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
SVM	Support Vector Machine
SMOTE	Synthetic Minority Over-sampling Technique
DoS	Denial of Service
PCA	Principal Component Analysis

INTRODUCTION GÉNÉRALE

1. Contexte et problématique

Initié par Kevin Ashton [1], l'Internet des Objets (IoT) redéfinit la façon dont nous interagissons avec le monde qui nous entoure. L'IoT nous facilite la vie en améliorant la qualité de vie et l'efficacité opérationnelle dans divers secteurs tels que la santé, l'industrie et la gestion domestique en transformant les objets conventionnels en systèmes interactifs et autonomes [2][3].

Cette croissance rapide de l'IoT révèle de grave vulnérabilité en matière de sécurité des données [4]. Des incidents récents tels que les attaques sur les réseaux de caméras de surveillance et les systèmes de contrôle domestique ont démontré que les failles de sécurité mettent en péril la fiabilité de l'IoT [5]. Les attaques DoS sont particulièrement alarmantes car elles peuvent perturber et même paralyser les réseaux [7][8]. Ces attaques visent à surcharger le réseau avec un trafic excessif, empêchant donc les appareils IoT à répondre aux demandes légitimes résultats occasionnant des dégâts dévastateurs pour des secteurs critiques tels que les infrastructures industrielles et les systèmes de santé connectés [7]. La sécurisation des informations échangées est donc très importante pour garantir la disponibilité et la sécurité globale des utilisateurs en raison des milliards de dispositifs connectés [9]. Ces événements mettent en lumière l'importance cruciale de développer des mécanismes de protection robustes contres ce type d'attaques, adaptés à la complexité et à la diversité de l'Internet des objets [10].

Dans ce contexte, le développement des méthodes efficaces de détection d'intrusions visant le répertoriage des comportements suspects et malveillants dans les réseaux devient cruciale pour protéger les infrastructures IoT [11]. Cependant, les méthodes traditionnelles

de détection d'intrusion sont peu adaptées aux particularités de l'IoT telles que la diversité des appareils et des protocoles, ainsi que leurs contraintes de traitements et de stockage[11][12].Il est donc nécessaire de recourir à des approches plus avancés et sophistiqués soulignant ainsi le potentiel de l'apprentissage automatique pour développer des systèmes capables de contrer efficacement les nouvelles menaces et pallier à l'insuffisances des méthodes traditionnelles.

2. Objectifs et sous-objectifs

L'objectif principale visé par ce travail de recherche est d'identifier un modèle d'apprentissage destiné à détecter efficacement les attaques DoS dans les systèmes IoT .

Pour atteindre cet objectif, notre démarche se divise en deux sous-objectifs :

- Identifier des modèles et des combinaisons pouvant permettre de détecter efficacement les attaques DoS dans les systèmes IoT
- Obtenir des prédictions avec un faible taux de faux positifs et comparer les performances de notre modèle avec celles des approches de détection traditionnelles et récentes pour démontrer son efficacité

A travers ces objectifs, notre recherche contribue à renforcer la sécurité des systèmes IoT en intégrant des approches adaptées pour améliorer la détection d'intrusion.

3. Méthodologie

Dans cette étude, nous avons utilisé une méthodologie, présentée dans la Figure 1, visant à améliorer la détection des attaques DoS au sein des systèmes IoT grâce à l'application de techniques de ML. Nous avons débuté notre approche en choisissant et en prétraitant l'ensemble de données Edge IIoT, ce qui impliquait l'encodage des fonctionnalités catégorielles, la suppression de données non pertinents et la normalisation l'ensemble de données pour garantir l'uniformité de la contribution des fonctionnalités. Compte tenu du large éventail de types d'attaques et du volume important d'enregistrements de trafic réseau,

il était essentiel d'appliquer l'équilibrage des classes et des techniques de sélection de caractéristiques pour répondre efficacement à sa complexité et à sa variabilité.

Pour l'équilibrage des classes, nous avons utilisé la technique de suréchantillonnage des minorités synthétiques (SMOTE) et le sous-échantillonnage aléatoire (Random Undersampling) améliorant ainsi la capacité du modèle à identifier avec précision les attaques DoS.

La sélection des caractéristiques est bénéfique pour améliorer les performances du modèle. La présence de caractéristiques non pertinentes peut diluer les informations utiles et entraver la capacité du modèle à distinguer efficacement les activités normales des attaques. Pour isoler les caractéristiques les plus importantes pour la détection des attaques, les DNN, Random Forest [34] et PCA ont été utilisées pour la sélection des caractéristiques. Pour la classification, nous avons intégré quatre modèles distincts : SVM, DNN, XGBoost et Random Forest, chacun affiné grâce à des techniques d'optimisation d'hyperparamètres spécifiques.

Il est crucial d'évaluer l'impact de chaque technique sur les performances du modèle pour déterminer la combinaison la plus appropriée pour notre cas spécifique. Ainsi, différentes combinaisons de techniques (sélection de fonctionnalités, équilibrage des classes, classification). Ces modèles ont été évalués en utilisant des mesures telles que la précision, le rappel, le score F1 et l'exactitude, ainsi que des outils analytiques tels que des matrices de confusion, des courbes ROC et une validation croisée stratifiée pour vérifier leur efficacité dans la détection des attaques DoS.

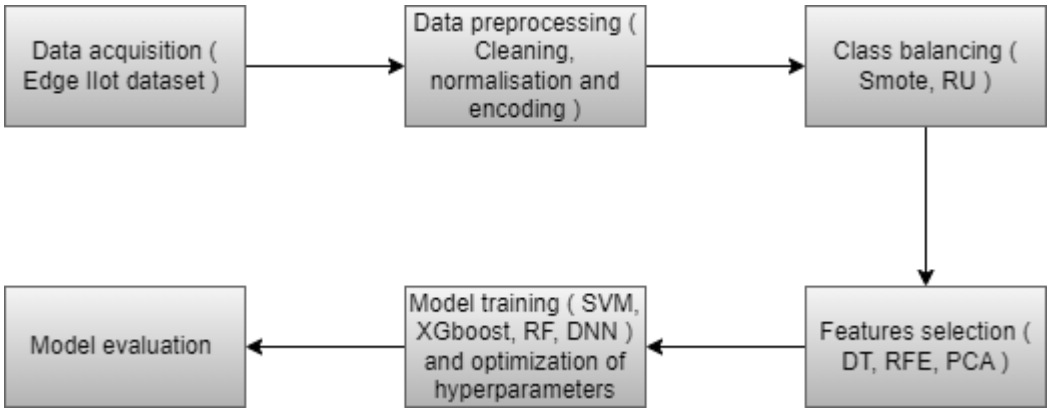

Figure 1 : Résumé de la méthodologie

4. Contributions

Cette recherche apporte deux contributions principales. La première est une revue systématique de la littérature sur les approches d'apprentissage automatique pour la détection des intrusions dans les systèmes IoT couvrant les méthodes supervisées, non supervisées, d'apprentissage profond, ainsi que les modèles combinant diverses méthodes [13

La seconde contribution est le développement d'une méthodologie intégrant des techniques d'équilibrage de classes, de sélection de caractéristiques et de classification quidémontre l'efficacité de différentes combinaisons de ces techniques pour une détection des attaques DoS[14]. Ces résultats contribuent à l'avancement des méthodes de sécurité dans les systèmes IoT en fournissant des comparaisons précises pour la mise en œuvre de techniques d'apprentissage automatique efficaces.

Deux articles scientifiques ont été accepté et publié dans le cadre de ce travail. Le premier article[13] publié dans le journal MDPI porte sur la revue systématique de la littérature détaillant les techniques existantes et les challenges dans la détection des attaques dans les systèmes IoT. Le second article[14] et publié dans la conférence "MOBISPC 2024", complète les contributions de ce mémoire avec des analyses détaillées, des résultats

expérimentaux et des recommandations pratiques dans le domaine de la sécurité des systèmes IoT

5. Organisation du mémoire

Ce mémoire suit la structure d'un mémoire par articles et est composé de quatre chapitres

Le premier chapitre plonge directement dans le vif du sujet, établissant le contexte et la pertinence des systèmes IoT dans notre société actuelle tout en soulignant les défis sécuritaires qu'ils engendrent. Il définit la problématique, les objectifs de la recherche, et offre une vue d'ensemble de l'organisation du mémoire, posant ainsi les bases de notre exploration.

Suivant cette introduction, le mémoire se penche sur une revue de littérature exhaustive présenté à travers un article, scrutant les travaux antérieurs relatifs à la sécurité des systèmes IoT, aux stratégies de détection d'intrusion et à l'apport potentiel de l'apprentissage automatique. Cette analyse critique permet non seulement de situer notre travail au sein du domaine académique existant mais aussi de mettre en exergue les lacunes que notre recherche vise à combler [13].

Le cœur du mémoire réside dans l'exposition de notre méthodologie, des résultats obtenus et de leur analyse critique. Cette section présente un article dans lequel nous montrons la méthodologie employée pour concevoir et évaluer notre modèle d'apprentissage hybride. En détaillant les choix méthodologiques, de la sélection des techniques d'apprentissage à la mise en œuvre du modèle, cette partie met en lumière la rigueur scientifique de notre démarche et la validité des processus employés pour parvenir à des résultats fiables [14].

Enfin, le quatrième chapitre conclut le mémoire avec un résumé des objectifs de ce projet de recherche ainsi qu'un bilan sur le travail accompli. Il discute des implications de nos recherches, tant sur le plan théorique que pratique, adresse les limites de l'étude et présente les perspectives.

CHAPITRE 1
REVUE DE LITTERATURE SUR LES METHODES DE DETECTION D'INTRUSION BASEES SUR L'APPRENTISSAGE AUTOMATIQUE DANS LES SYSTEMES IOT.

1.1 RÉSUMÉ EN FRANÇAIS DE L'ARTICLE 01 : MACHINE LEARNING-BASED INTRUSION DETECTION METHODS IN IOT SYSTEMS: A COMPREHENSIVE REVIEW[13]

Cet article examine en détail la sécurité des systèmes IoT, en commençant par une présentation de l'IoT, de sa croissance et de son architecture de base, avant d'aborder les problèmes et défis liés à leur sécurité, notamment les vulnérabilités et les attaques potentielles. L'article explore ensuite les diverses approches d'apprentissage automatique pour la détection des intrusions dans les systèmes IoT, y compris les méthodes d'apprentissage supervisé, non supervisé et profond. L'efficacité, les limites et les applications concrètes de ces techniques sont analysées, mettant en évidence le potentiel de l'apprentissage automatique pour renforcer la sécurité des systèmes IoT. L'étude aborde également les questions et les tendances actuelles dans le secteur, soulignant la nécessité d'une recherche et d'un développement continus pour rester à jour dans l'écosystème de la sécurité de l'IdO, qui évolue rapidement.

1.2 MACHINE LEARNING-BASED INTRUSION DETECTION METHODS IN IOT SYSTEMS: A COMPREHENSIVE REVIEW[13]

electronics

MDPI

Review

Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review

Brunel Rolack Kikissagbe * and Meddi Adda *

Mathematics, Computer Science and Engineering Departement, University of Quebec at Rimouski, Rimouski, QC G5L 3A1, Canada
* Correspondence: kikb0001@uqar.ca (B.R.K.); mehdi_adda@uqar.ca (M.A.)

Abstract: The rise of the Internet of Things (IoT) has transformed our daily lives by connecting objects to the Internet, thereby creating interactive, automated environments. However, this rapid expansion raises major security concerns, particularly regarding intrusion detection. Traditional intrusion detection systems (IDSs) are often ill-suited to the dynamic and varied networks characteristic of the IoT. Machine learning is emerging as a promising solution to these challenges, offering the intelligence and flexibility needed to counter complex and evolving threats. This comprehensive review explores different machine learning approaches for intrusion detection in IoT systems, covering supervised, unsupervised, and deep learning methods, as well as hybrid models. It assesses their effectiveness, limitations, and practical applications, highlighting the potential of machine learning to enhance the security of IoT systems. In addition, the study examines current industry issues and trends, highlighting the importance of ongoing research to keep pace with the rapidly evolving IoT security ecosystem.

Keywords: IoT; security; intrusion detection; machine learning; DoS

Citation: Kikissagbe, B.R.; Adda, M. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. *Electronics* **2024**, *13*, 3601. https://doi.org/10.3390/electronics13183601

Academic Editors: Giovanni Pau and Xiangjie Kong

Received: 3 May 2024
Revised: 2 September 2024
Accepted: 4 September 2024
Published: 11 September 2024

1. Introduction

In the ever-evolving field of information technology, the Internet of Things (IoT) has emerged as a groundbreaking innovation, integrating everyday objects into the Internet, making our environment more interactive and automated [1]. However, with the exponential growth of IoT, significant security challenges have also emerged, attracting the attention of researchers and industry professionals [2].

Intrusion detection systems (IDSs) play a crucial role in protecting computer systems by detecting and responding to malicious activities. They continuously monitor networks to identify abnormal behaviors or potential attacks, thereby maintaining the integrity, confidentiality, and availability of systems. Traditional IDS methods, designed for standard networks, face major challenges in diverse IoT networks [3]. Their lack of flexibility regarding the variety of IoT devices and protocols reduces their effectiveness. Advanced attacks, including zero-day attacks, easily surpass these IDSs, which rely on known signatures. Additionally, their inability to process large volumes of data leads to performance and scalability issues. Their dependence on manual signature updates increases the vulnerability of IoT systems. Traditional IDSs also struggle to differentiate legitimate behaviors from malicious ones in varied IoT traffic patterns, thus increasing the risk of errors.

In response to these limitations, machine learning has emerged as a promising solution capable of adapting and responding to complex and evolving threats in the IoT environment [4]. Machine learning-based IDSs can learn from historical data to detect abnormal behaviors, offering an enhanced ability to identify new and unknown attacks. Furthermore, these systems can process large volumes of data and continuously improve through machine learning.

This review delves into various machine learning approaches, including supervised, unsupervised, and deep learning methods, evaluating their effectiveness in intrusion detection. The discussion also covers practical applications and industry implications, highlighting the importance of ongoing research to enhance IoT system security. By providing a comparative analysis of existing methods, this review aims to identify the best practices and current gaps to guide future research.

The core of this review focuses on intrusion detection systems in IoT, exploring the basic principles, significance, and traditional detection methods. It then analyzes the limitations of these traditional approaches and presents machine learning as a possible solution. The subsections detail supervised, unsupervised, and deep learning, evaluating their effectiveness and limitations in the context of IoT systems. Finally, the review concludes with a discussion on emerging trends and challenges in intrusion detection for IoT and offers a critical analysis of current methods as well as suggestions for future research.

2. Materials and Methods

A systematic review is an explicit and reproducible research methodology that identifies all relevant studies and summarizes the state of the art, in order to answer one or more fundamental research questions on a particular topic. In this section, we will present the detailed methodology used to conduct our systematic review of machine learning-based intrusion detection methods in IoT systems. Our approach follows the guidelines described in the PRISMA (preferred reporting items for systematic reviews and meta-analyses) method.

2.1. Eligibility Criteria

To ensure that only the most relevant studies were included in this systematic review, we defined specific inclusion and exclusion criteria. These criteria were systematically applied when evaluating each article identified in our initial search. The Table 1 below summarizes these criteria:

Table 1. Eligibility criteria for the systematic review.

Criterion	Description
Language	Only articles written in English.
Period	Only articles published in the last 10 years (between January 2014 and May 2024) due to the rapid developments in the field of IoT security.
Main topic	Only articles with the main topic of intrusion detection in IoT systems.
Techniques	Only articles addressing the topic with machine learning (ML)-based techniques.
Evaluation	Only peer-reviewed articles published in recognized scientific journals.

Scientific interest in the use of machine learning has grown over the past decade. The articles included in this review were published between 2013 and 2024. The following two graphs show the evolution of research over the last few years. Figure 1 shows the distribution of literature and systematic reviews on the subject over the last 5 years, while Figure 2 shows the evolution of publications relevant to our study over the last 10 years.

2.2. Data Sources and Search Strategy

Data Sources

For the identification and collection of articles related to our research, a literature search was performed across several electronic databases, including IEEE Xplore, PubMed, Scopus, and Google Scholar. These databases were selected for their relevance to the topic and scope of the search. Fields considered in search queries included the title, abstract, and keywords. Searches were formulated using several keywords corresponding to the eligibility criteria and using Boolean operators (AND, OR, NOT) to efficiently query the scientific publication databases. In addition, additional articles were identified from the bibliographies of the included articles. The Table 2 summarizes the queries launched in the various databases cited.

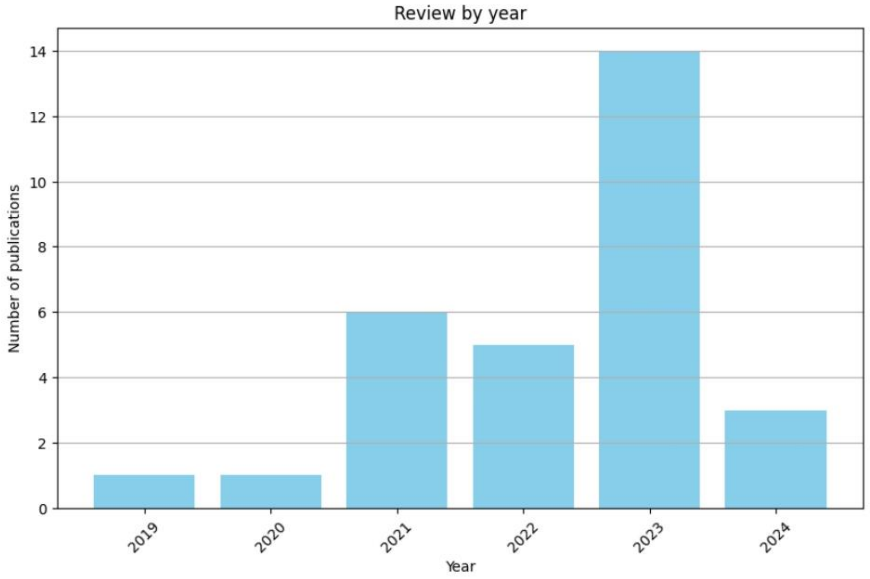

Figure 1. Distribution of reviews over the past 5 years (PubMed Database).

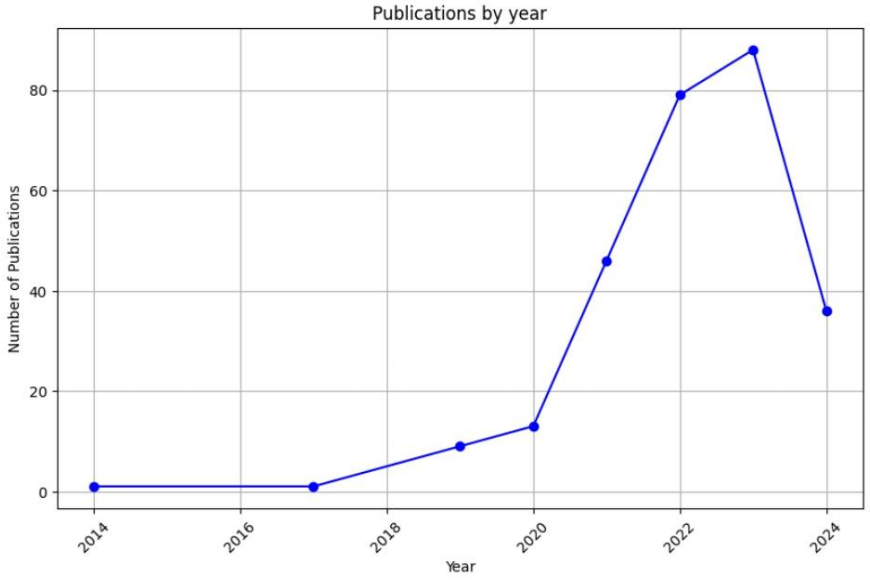

Figure 2. Distribution of documents by year (PubMed database).

Table 2. Search queries for databases.

Database	Search Query
IEEE Xplore	(”IoT” OR ”Internet of Things”) AND (”intrusion detection” OR ”anomaly detection” OR ”cybersecurity”) AND (”machine learning” OR ”artificial intelligence” OR ”deep learning” OR ”KNN” OR ”SVM” OR ”GAN” OR ”ANN” OR ”logistic regression” OR ”Random Forest”) AND (LIMIT-TO (PUBYEAR, 2014–2024)) AND (LIMIT-TO (LANGUAGE, ”English”))
PubMed	((”IoT” OR ”Internet of Things”) AND (”intrusion detection” OR ”anomaly detection” OR ”cybersecurity”) AND (”machine learning” OR ”artificial intelligence” OR ”deep learning” OR ”KNN” OR ”SVM” OR ”GAN” OR ”ANN” OR ”logistic regression” OR ”Random Forest”) AND (”2014/01/01”[PDAT]: ”2024/05/31”[PDAT]) AND English[lang])
Scopus	TITLE-ABS-KEY ((”IoT” OR ”Internet of Things”) AND (”intrusion detection” OR ”anomaly detection” OR ”cybersecurity”) AND (”machine learning” OR ”artificial intelligence” OR ”deep learning” OR ”KNN” OR ”SVM” OR ”GAN” OR ”ANN” OR ”logistic regression” OR ”Random Forest”)) AND NOT (DOCTYPE (”re”)) AND PUBYEAR > 2013 AND PUBYEAR < 2025 AND (LIMIT-TO (LANGUAGE, ”English”))
Google Scholar	(”IoT” AND ”intrusion detection” AND ”cybersecurity”) AND (”machine learning” OR ”artificial intelligence” OR ”deep learning” OR ”KNN” OR ”SVM” OR ”GAN” OR ”ANN” OR ”logistic regression” OR ”Random Forest”) AND (LIMIT-TO (PUBYEAR, 2014–2024)) AND (LIMIT-TO (LANGUAGE, ”English”))

2.3. Search Strategy

We searched the IEEE Xplore, PubMed, Scopus, and Google Scholar databases using specific search terms to capture relevant articles. Fields considered in the search queries included the title, abstract, and keywords. Searches were formulated using several keywords corresponding to the eligibility criteria and using Boolean operators (AND, OR, NOT) to efficiently query scientific publication databases. The search terms used for each category were as follows:

- IoT: ”IoT”, ”Internet of Things”, ”IoT system”.
- Intrusion detection: ”intrusion detection”, ”anomaly detection”, ”cybersecurity”.
- Machine learning: ”machine learning”, ”artificial intelligence”, ”ML”, ”AI”, ”deep learning”, ”supervised learning”, ”unsupervised learning”, ”neural network”, ”random forest”, ”support vector machine”, ”SVM”, ”Random Forest”, ”Decision Tree”, ”DNN”, ”ANN”, ”KNN”, ”GAN”, ”logistic regression”, ”ANN”.
- Challenges: ”security challenges”, ”IoT security issues”, ”cybersecurity challenges”, ”AI challenges”, ”threat detection challenges”, ”IoT vulnerabilities”, ”AI limitations in IoT security”.

2.4. Study Selection

We used a reference management tool to record the references, eliminate duplicates, and create a unique database of references after querying the databases. To select articles from the initial database, we applied a three-step process.

- Title evaluation;
- Abstract and keyword evaluation;
- Full-text evaluation.

The aim was to remove irrelevant studies during steps (1) and (2), and then review the remaining documents using the eligibility criteria specified in step (3). Finally, during the eligibility phase, we compiled the included studies into our final database and noted the main reasons for excluding other articles based on the given criteria.

The entire flowchart of the selection process, including identification, screening, eligibility, and inclusion, is shown in Figure 3.

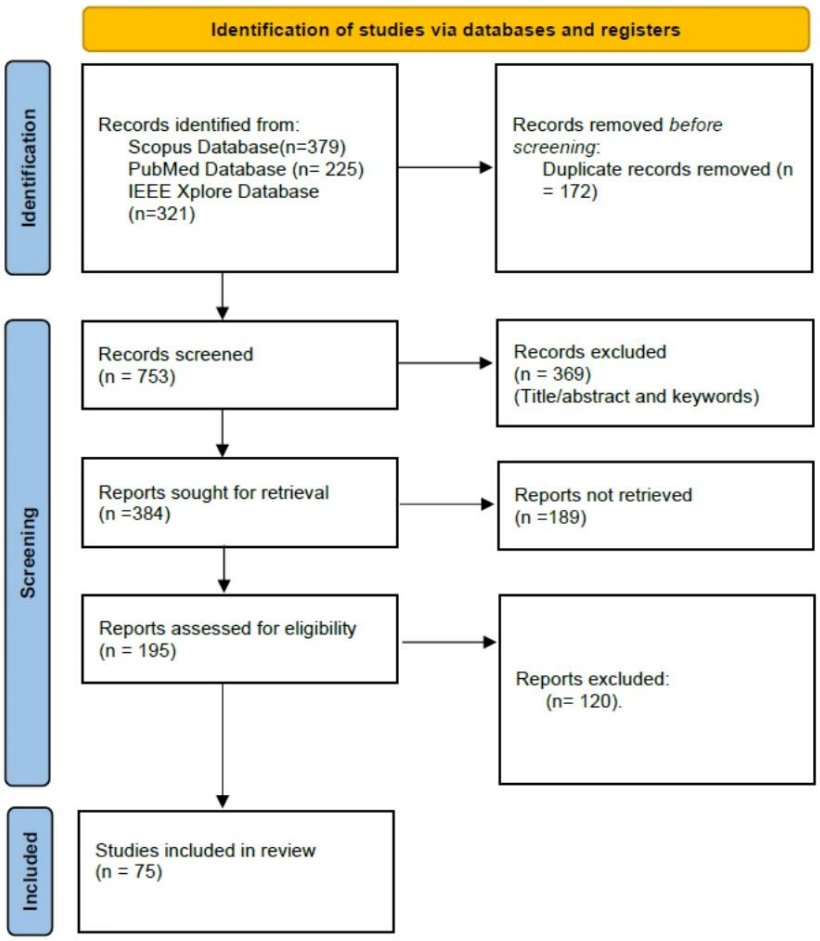

Figure 3. The PRISMA flow diagram.

3. Internet of Things

3.1. Definition and Growth of IoT

The Internet of Things (IoT) is a concept that has gained momentum in the early 21st century. According to Ashton [1], who is credited with introducing the term, IoT refers to a network of physical objects equipped with sensors, software, and other technologies, enabling them to connect and exchange data with other devices and systems over the Internet. This definition highlights the transformation of ordinary objects into "smart" entities capable of autonomous communication and interaction.

We will present the various definitions attributed to the Internet of Things as they appear in the literature.

According to the International Telecommunication Union [5], the Internet of Things is defined as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". This definition emphasizes the interconnection of objects and the exploitation of their capabilities to offer various services while ensuring security and privacy.

According to Corici et al. [6], the Internet of Things is an evolving field in which hardware and software components model, sense, or influence properties of the physical world. To exploit the potential of an IoT service, security and flexibility are essential requirements.

Sha et al. [7] described the Internet of Things as an emerging paradigm, considering it as the third major wave of innovation in the field of information technology, succeeding the Internet and mobile computing technology. Reference [8] presented compelling data confirming strong growth in the IoT market. Their analysis revealed an exponential increase, forecasting a value reaching several billion US dollars. In addition, the study detailed the progress of IoT in various economic sectors. Significant growth in the automotive, healthcare, and lifestyle fields highlights the widespread expansion of IoT into practical applications that influence our daily lives. Furthermore, Gormus et al. [9] added another dimension to our understanding by explicitly showing the diverse sectors covered by the IoT. This broad coverage confirms that the IoT is everywhere, transforming many sectors of the economy and society. In healthcare, the IoT has introduced remote monitoring systems and connected medical devices that enable continuous monitoring and optimization of care decisions. These advances, supported by the work of Ibrahim et al. [10], promote proactive health management with rapid, secure access to medical records. In the urban planning sector, the impact of IoT is embodied by the development of smart cities. The integration of a network of sensors and actuators, as demonstrated in the study by Pérez and Rodriguez [10], enables efficient management of urban resources, optimizing environmental parameters such as temperature and humidity. This improved management translates into a higher quality of life for city dwellers. In addition, the IoT has also proved its usefulness in the creation of Smart Homes adapted to people with disabilities, a concept put forward by Hussein et al. [11]. These smart homes, designed to meet the specific needs of individuals, illustrate the personalized and humanized application of the IoT. This information, consolidated by IDC [8] forecasts of 41.6 billion connected IoT devices by 2025, underlines the scale of the phenomenon. As the cornerstone of modern societies, the IoT is at the heart of the synergy between technology and infrastructure, propelling our societies into an era of increased connection and intelligence. The rapid expansion of IoT technology can be explained by several factors. Perera et al. [2] identified the evolution of wireless technologies, increased Internet bandwidth, and reduced technology costs as key drivers of IoT growth. In addition, Atzori et al. [12] highlighted the importance of interoperability in IoT, enabling heterogeneous devices to collaborate and paving the way for innovative applications and enhanced services.

3.2. Basic Architecture of IoT

The architecture of the Internet of Things (IoT) is often described in terms of layers to simplify its understanding and development. Although there is no single architecture standard, and developing one is complex due to the natural fragmentation of potential applications, we can conceptualize it in three main layers: the perception layer, the network layer, and the application layer [13].

The perception layer is responsible for collecting physical information using sensors, RFID, GPS, and other devices, converting it into digital data for processing and analysis [14].

The network layer handles data transmission and processing, efficiently transmitting data collected by the perception layer to information processing devices, including cloud servers. It uses various communication protocols such as Wi-Fi, Bluetooth, Zigbee, LoRa, and others [15].

The application layer delivers practical, interactive services and solutions in fields such as healthcare, home automation, and energy management, making IoT tangible for end-users.

This three-layer structure Figure 4 simplifies the complexity of IoT systems and enables a better understanding of their operation and management. It also highlights the importance of harmonious integration between layers to ensure optimal efficiency and security of IoT systems.

In our study, we will use this basic architecture of IoT systems as the basis for our analysis.

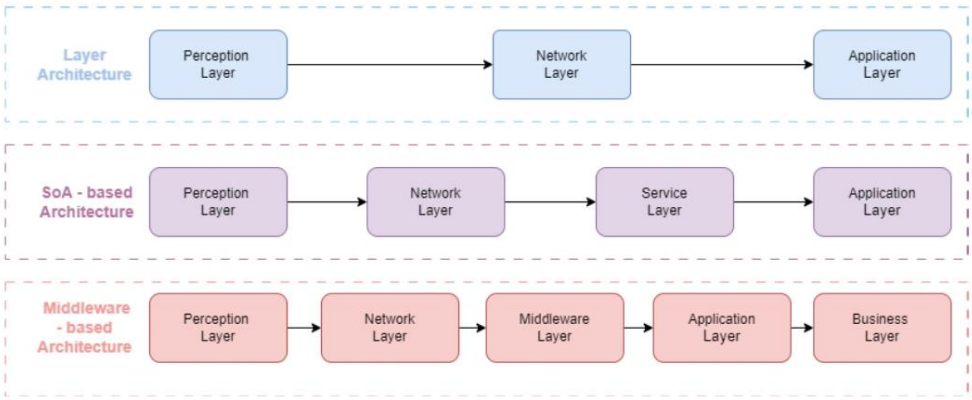

Figure 4. Common IoT architectures.

4. Classification of IoT Attacks Based on Vulnerabilities and Layers

In this section, we present a comprehensive classification of IoT attacks by examining both the vulnerabilities they exploit and the specific layers of the IoT architecture they target. This dual classification is essential for comprehensively understanding potential threats and developing more effective defense strategies.

4.1. Categorization of Vulnerabilities

IoT systems exhibit several vulnerabilities, which can be categorized based on the different layers of the IoT architecture:

4.1.1. Physical Layer

The security of connected objects presents several significant challenges, such as resource constraints and data storage vulnerabilities [6,16–18]. Jing et al. [18] highlighted the physical vulnerability of IoT devices, noting that direct access to devices can lead to serious security breaches, especially when placed in public or unmonitored areas [19].

Hardware limitations make it difficult to implement effective security measures, and vulnerabilities in securing locally stored data pose significant risks [12,15].

4.1.2. Network Layer

The network layer faces vulnerabilities related to insecure communication protocols, diverse connectivity standards, and weak authentication mechanisms [11,16]. Insecure default configurations and insufficient network segmentation further increase the risk of unauthorized access [15].

4.1.3. Application Layer

Application layer vulnerabilities include a lack of updates, third-party application risks, and weaknesses in cryptographic implementations [12,16]. Neglect in updating security patches and the use of weak passwords facilitate unauthorized access, highlighting the need for robust authentication and authorization systems [15].

We introduce a taxonomy Figure 5 that allows us to visualize these vulnerabilities by layer.

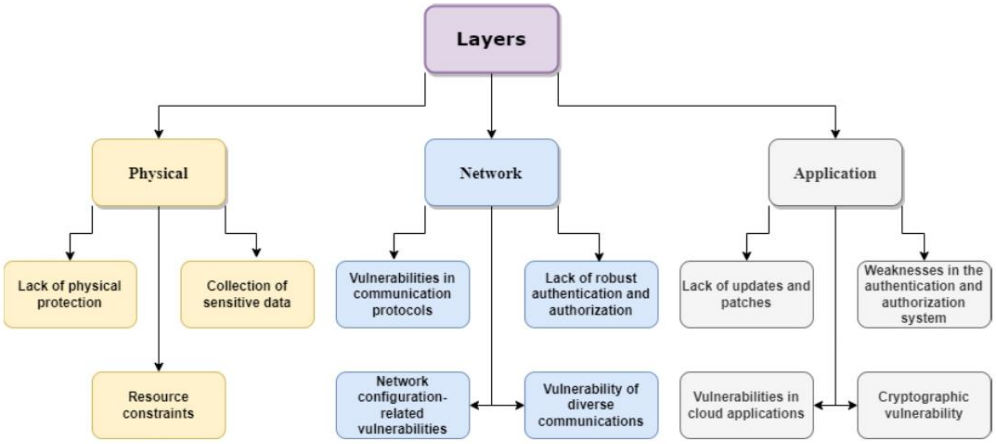

Figure 5. Classification of vulnerabilities by layer.

4.2. Categorization of Attacks

There are multiple attacks on IoT and IIoT objects, which can be classified according to vulnerabilities or according to layers.

4.2.1. Perception Layer

Attacks at the perception layer, such as sensor tampering and side-channel attacks, compromise the integrity of collected data and the functioning of IoT devices [20–22]. Physical attacks like destruction or theft further threaten device security [23].

4.2.2. Network Layer

The network layer is vulnerable to DoS, DDoS, and identity spoofing attacks, which disrupt communication and access to services [14,21,22,24]. Man-in-the-middle and sniffing attacks also compromise the confidentiality and integrity of data exchanges [22].

4.2.3. Application Layer

Application layer attacks include code injection, ransomware, and data theft, targeting the security and availability of IoT applications [16]. Buffer overflows and social engineering further highlight the need for secure development practices and user awareness [12].

Below, we present a Figure 6 summarizing all the layer attacks.

Following the previous classification of attacks by layers in IoT systems, we have developed a detailed taxonomy Figure 7 that organizes these attacks based on the specific vulnerabilities they exploit. This structuring allows us to clearly illustrate the direct links between vulnerabilities inherent in IoT technologies and the various types of attacks identified.

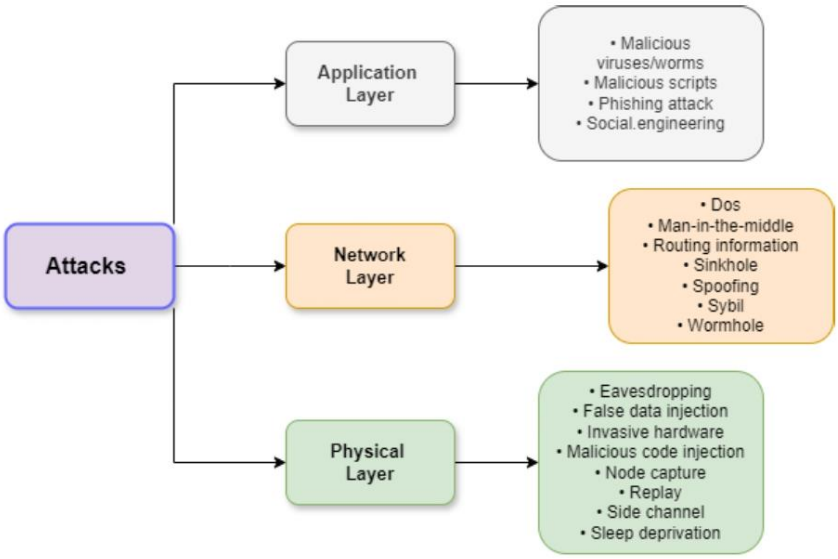

Figure 6. Classification of attacks by layers.

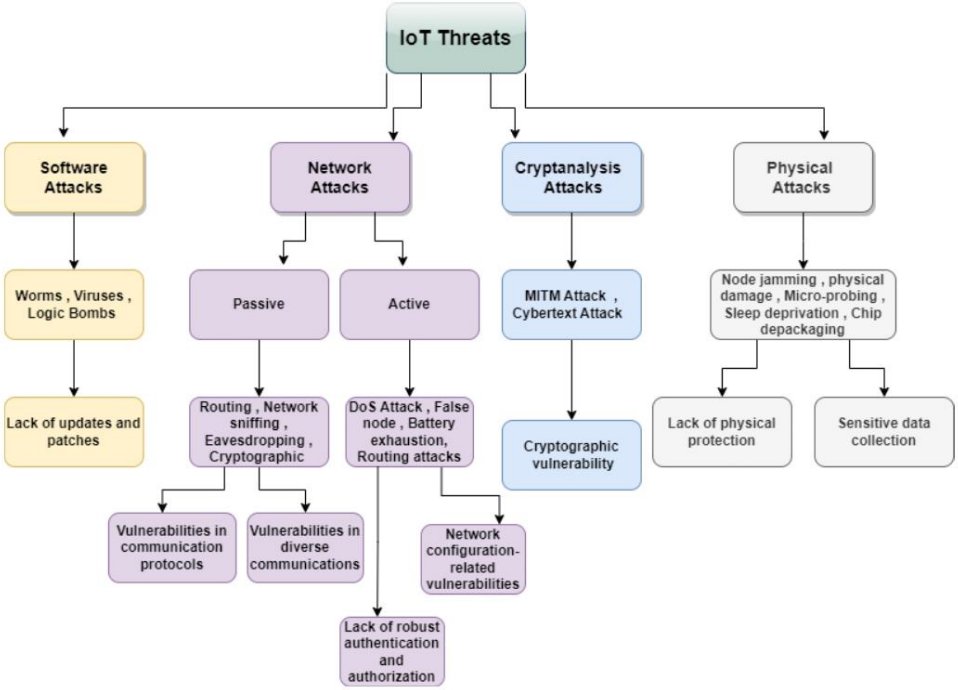

Figure 7. Taxonomy of attack classification according to vulnerabilities.

5. Traditional Intrusion Detection Methods

Intrusion detection systems (IDSs) are essential tools for identifying potential threats and ongoing attacks in IoT systems. Traditional detection methods can be divided into two main categories based on the source of the analyzed data and the detection method.

5.1. Classification Based on Data Source

Among the methods based on data sources, IDSs can be divided into host-based (HIDS) and network-based (NIDS) methods.

NIDSs (network intrusion detection systems), as described by Liu and Lang [25], monitor overall network traffic to detect malicious or suspicious activities. They analyze packets circulating through the network for malicious behaviors or anomalies. These NIDSs can detect attacks occurring between IoT devices and network nodes, and they are effective in identifying suspicious activities that may go unnoticed at the individual host level. The majority of network-based IDSs are independent of the operating system; thus, they can be applied in different operating system environments. The disadvantage is that they only monitor traffic passing through a specific network segment.

HIDSs (host intrusion detection systems), on the other hand, are host-based systems installed on individual IoT or IIoT devices. They monitor host-specific activities and behaviors, such as file changes, unauthorized access attempts, or abnormal operating system behaviors. HIDSs can detect attacks targeting a specific IoT device or resource, providing additional protection at the local level [25]. The drawbacks are that host-based IDSs consume host resources, depend on host reliability, and are unable to detect network attacks.

Hybrid deployment-based detection systems combine both network-based (NIDS) and host-based (HIDS) deployment elements. This approach allows for the benefits of both methods and enhances the overall system security. The Table 3 summarizes the difference between NIDS and HIDS.

Table 3. Comparison between NIDS and HIDS.

Criteria	NIDS	HIDS
Surveillance type	Global network traffic surveillance	Surveillance of specific host activities
Data source	Network traffic	Operating system or application program logs
Detection scope	Malicious or suspicious activities in network traffic	File modifications, unauthorized access attempts, abnormal system behaviors [25]
Operating system independence	Independent of the host operating system	Dependent on the host operating system
Detection target	Attacks between IoT devices and network nodes	Attacks specifically targeting an IoT device or resource [25]
Detection efficiency	High, can detect real-time attacks	Low, needs to process numerous logs [25]
Intrusion traceability	Traces intrusion position and time-based on IP addresses and timestamps	Traces intrusion process based on system call paths
Limitation	Monitors only traffic passing through a specific network segment	Cannot analyze network behaviors

5.2. Classification Based on Detection Method

Several intrusion detection methods are used to detect intrusions in the IoT and IIoT domains.

Anomaly-based method.

The first method is based on behavior modeling, detecting anomalies that correspond to abnormal behavior. This method uses statistical models to establish a baseline of normal behavior for IoT devices. By continuously monitoring data flows, traffic patterns, and communication schemes, the system can detect anomalies that may indicate suspicious or malicious activity. For example, if an IoT device starts generating abnormally high traffic volume or communicating with unusual destinations, this could indicate an intrusion attempt. According to Liu and Lang [25], anomaly detection is particularly useful for identifying unknown attacks and new or emerging behaviors.

Misuse-based or signature-based method.

Misuse detection, also known as signature-based detection, relies on representing attack behaviors as signatures. The detection process involves comparing the signatures of samples with a signature database. The main challenge in building misuse detection systems is designing effective signatures. The advantages of misuse detection lie in its low false alarm rate and its ability to provide detailed information about attack types and their possible reasons. As highlighted by Liu and Lang [25], it has disadvantages such as a high rate of missed alarms, the inability to detect unknown attacks, and the need to maintain a large signature database. In contrast, anomaly detection is based on establishing a profile of normal behavior and then identifying abnormal behaviors based on their deviation from this profile. Thus, the key to designing an anomaly detection system lies in clearly defining a normal profile. The advantages of anomaly detection are its high generalization ability and its ability to recognize unknown attacks. However, it has disadvantages such as a high rate of false alarms and the inability to provide possible reasons for an anomaly. Here Table 4 is a comparison table between anomaly-based and signature-based intrusion detection methods:

Table 4. Comparison between anomaly-based and signature-based methods.

Criteria	Anomaly-Based Method	Signature-Based Method (Misuse Detection)
Operating principle	Modeling normal behavior and detecting deviations	Representing attack behaviors as signatures
Detection approach	Monitoring data flows, traffic models, and communication patterns	Comparing samples with a signature database
Effectiveness against unknown attacks	High	Low
False positive management	High false alarm rate	Low false alarm rate
Attack information	Unable to provide precise reasons for detected anomalies	Provides detailed information on attack types and possible reasons
Main challenges	Clearly defining a normal behavior profile	Designing effective signatures
Advantages	High generalization capability, recognizes unknown attacks [25]	Low false alarm rate, detailed information on attacks
Disadvantages	High false alarm rate, difficulty in identifying reasons for anomalies	High rate of missed alarms, unable to detect unknown attacks, need to maintain a large signature database

5.3. Limits of Traditional Approaches and Comparison with Machine Learning-Based IDS

Traditional intrusion detection systems (IDSs), designed for standard networks, face significant challenges in diverse IoT networks [3]. Their lack of flexibility toward the variety of IoT devices and protocols reduces their effectiveness. Advanced attacks, including zero-day attacks, easily surpass these IDS, which rely on known signatures. Additionally, their inability to handle large volumes of data leads to performance and scalability issues. Their dependency on manual signature updates increases the vulnerability of IoT systems. Traditional IDSs also struggle to differentiate between legitimate and malicious behaviors in varied IoT traffic patterns, increasing the risk of errors. Privacy concerns and integration challenges with IoT further complicate their use. These limitations indicate the need for approaches more suited to IoT.

In contrast, machine learning-based IDSs offer more flexible, scalable, and intelligent solutions to combat security threats in IoT. The Table 5 compares the two approaches:

Machine learning-based IDSs can adapt to new behaviors and traffic patterns, making them more suitable for the dynamic and diverse nature of IoT environments. While they may have a higher false positive rate, this can be managed with careful tuning and continuous learning. By integrating these more advanced techniques, IoT systems can achieve a higher level of security, effectively addressing the limitations of traditional IDS.

Table 5. Comparison between traditional and machine learning-based IDSs.

Criteria	Traditional IDS	Machine Learning-Based IDS
Flexibility	Limited, depends on known signatures	High, can detect unknown behaviors
Scalability	Limited, performance issues with large data volumes	Good, handles large data with appropriate resources
Dependency on updates	High, requires manual signature updates	Low, learns continuously from new data
Detection of unknown attacks	Low, does not detect zero-day attacks	High, detects anomalies and new attacks
False positive rate	Low for known attacks, high for new ones	Variable, high for anomalies but manageable
Attack information	Detailed for known attacks	Limited but can be improved with interpretability techniques

6. Machine Learning for Intrusion Detection

In the field of intrusion detection, particularly in IoT systems, machine learning has established itself as a leading technology. This branch of artificial intelligence enables systems to automatically detect suspicious or malicious activity by learning from available data [26]. There are several approaches to machine learning for intrusion detection, each with its own strengths and limitations depending on the application context. Figure 8 presents the taxonomy of different machine learning methods used in IoT.

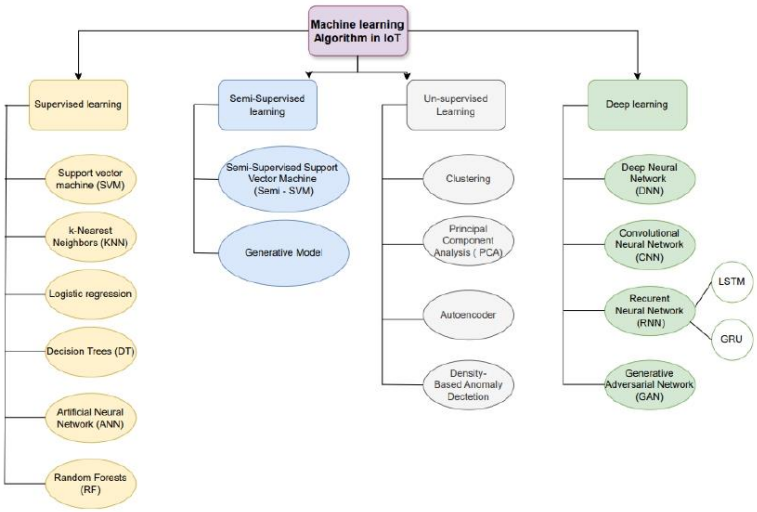

Figure 8. Taxonomy of machine learning methods in IoT.

7. Supervised Learning

Supervised learning relies on the use of labeled data, where each data point is associated with a label indicating whether it represents an intrusion or normal activity. The model learns to make this distinction by analyzing the features of the training data and is then able to predict labels for new data.

7.1. Popular Methods and Applications

7.1.1. Artificial Neural Networks (ANNs)

ANNs are trained to recognize specific attack signatures and abnormal behavior by analyzing network traffic [27]. According to research by Sohaib et al. [28], this method has demonstrated an average accuracy of 84% and a low false-positive rate, at less than 8%,

in repeated cross-validation for intrusion detection in IoT systems. Arul Anitha et al. [27] also proposed an artificial neural network-based intrusion detection system using a multilayer perceptron (MLP) approach to detect DOS and version attacks in IoT. They captured 73,880 data packets in their simulation, of which 1307 were malicious. The MLP model trained correctly classified malicious and normal packets, with a very low error rate. L. Jamal et al. [29] also used ANNs to detect malicious behavior on an IoT network dataset consisting of 461,043 records in total, of which 300,000 were benign and 161,043 were malicious. With the proposed methodology, malware was detected with an accuracy of 94.17% and classified with an accuracy of 97.08%. These results underline the ability of ANNs to efficiently process large heterogeneous datasets. However, a major challenge remains regarding the accurate distinction between malicious and normal data packets, especially in the case of large volumes of data processed by the ANN. The authors highlighted the effectiveness of their model in detecting intrusions with high accuracy while noting the need for more research to apply it to real data [27].

7.1.2. Support Vector Machine (SVM)

SVMs are widely used for intrusion detection in IoT systems. Goeschel et al. [30] demonstrated the effectiveness of SVMs, achieving an accuracy of 99.62% with a low false positive rate of 1.57%. Jing et al. [18] used SVMs for intrusion detection with the UNSW-NB15 dataset, implementing a nonlinear scaling method that improved accuracy to 85.99% for binary classification and 75.77% for multiclass classification. SVMs have also been applied to secure intelligent networks, efficiently detecting known and unknown attacks and outperforming traditional methods. Ioannou et al. [31] evaluated two SVM approaches (C-SVM and OC-SVM) for detecting network attacks in IoT systems. C-SVM showed classification accuracy of up to 100% with unknown data from the same network topology and 81% accuracy in an unknown topology, while OC-SVM achieved a maximum accuracy of 58%. These results confirm the potential of SVM as a robust tool for anomaly detection in IoT network security [32]. However, SVMs can be less flexible with highly varied and dynamic IoT data. Building and optimizing SVM models, especially for large and complex datasets, can be computationally expensive. Further research is needed to improve their accuracy in unknown environments.

7.1.3. K-Nearest Neighbors (KNNs)

K-Nearest Neighbor (KNN) is a non-parametric classification method effective for tasks such as intrusion detection in IoT systems [33,34]. Abdaljabar et al. [34] implemented an approach combining KNN and Decision Tree algorithms, achieving an accuracy of 100% after data normalization, proving effective in detecting IoT attacks. Wenchao Li et al. [35] developed a similar system for wireless sensor networks, focusing on accuracy and speed. Govindarajan et al. [36] adopted a hybrid k-NN method, incorporating cross-validation to improve performance, despite the lack of precision on the datasets used. Another study by Aref et al. [37] introduced a semi-supervised approach with hyper-parametric KNN using the NSL-KDD dataset, achieving 95% accuracy. These studies highlight the effectiveness of KNN in intrusion detection but also its limitations, such as sensitivity to the choice of the parameter 'k' and susceptibility to noise in the data.

7.1.4. Logistic Regression (LR)

Linear regression has been effectively used in identifying specific threats within IoT environments. Bapat et al. [38] used LR to identify malicious botnet traffic, demonstrating its usefulness in threat detection. Swathi Sambangi et al. [39] explored the use of multiple linear regression to detect DDoS attacks in cloud environments using the CIC-IDS 2017 dataset. They applied a feature selection technique to identify the most relevant attributes for predicting such attacks. The model achieved an accuracy of 73.79% using the 16 selected attributes, indicating its robustness for detecting DDoS attacks in cloud environments.

7.1.5. Decision Tree

Decision trees are highly effective in classifying and detecting abnormal behavior in IoT environments. Qaddoura et al. [40] used decision trees to examine network data flow, identifying suspicious traffic sources and helping to combat distributed denial-of-service (DDoS) attacks. Ingre et al. [41] developed an intrusion detection system (IDS) using a decision tree for the NSL-KDD dataset. They applied the correlation feature selection (CFS) method to enhance predictive performance, achieving high detection rates and accuracy, particularly in binary classification. Kajal Rai et al. [42] implemented the DT C4.5 algorithm for intrusion detection in IoT systems, focusing on feature selection and optimization. Using the NSL-KDD dataset, they reported satisfactory performance in terms of model building speed, false positive rate, true positive rate, and accuracy. However, the performance was influenced by dataset size and feature number. These studies demonstrate the adaptability and effectiveness of decision trees in complex applications. However, challenges such as difficulty in identifying new attack forms and dependence on proper feature selection can affect their accuracy in complex cybersecurity environments.

8. Unsupervised Learning

Unsupervised learning is a crucial approach in intrusion detection, particularly useful for identifying abnormal behaviors or anomalies in IoT systems. Unlike supervised learning, unsupervised learning does not rely on labeled data. Instead, it analyzes raw data to discover intrinsic patterns or groupings, which is especially beneficial when data labels are not available or are difficult to obtain.

8.1. Popular Methods and Applications

8.1.1. Clustering

Clustering is a fundamental technique in unsupervised machine learning. It involves grouping a set of data in such a way that the data in the same group (called a cluster) are more similar to each other than to data in other groups [43]. Common examples include K-means and hierarchical clustering [43]. In intrusion detection, these methods can identify clusters of similar behavior, enabling the detection of anomalous activity that deviates significantly from the established clusters. Muniyandi et al. [44] proposed an anomaly detection method combining K-means and the DT C4.5 algorithm. However, they found that the performance of K-means was less effective than that of supervised learning methods, particularly for the detection of known attacks. In parallel, Peng et al. [45] proposed an improved K-means-based detection method with a mini-batch for processing large datasets, such as the KDD99 dataset. K-means clustering has also been used to detect intrusions, specifically Sybil attacks in WSNs [35], with interesting results. This study suggests the use of channel vector clustering to distinguish Sybil attackers from normal sensors.

8.1.2. Principal Component Analysis (PCA)

PCA is a dimensionality reduction method that has been applied in IoT for efficient data processing. Peng et al. [45] used PCA on the KDD99 dataset, transforming features into numerical types before clustering them with improved K-means. This approach enhances clustering performance and reduces computational load. Zhao et al. [15] proposed a model using PCA for dimensionality reduction, combined with softmax regression and the KNN algorithm. Integrating PCA with these classifiers resulted in a system that is both efficient and low on computational resource demands, capable of operating in real-time in IoT environments.

However, PCA can lead to a loss of important information and assumes the linear independence of the principal components, which limits its application in some complex contexts.

8.1.3. Autoencoders

In the context of the Internet of Things (IoT), wireless sensor networks (WSNs) in particular, autoencoders have demonstrated their ability to solve complex problems. Luo et al. [46] proposed a model where autoencoders were introduced into WSNs to detect anomalies. This research implemented a two-part solution: anomaly detection on sensors in a distributed mode without the need for communication with other sensors or the cloud, and management of computationally intensive learning tasks on the IoT cloud. This case study illustrates how autoencoders can be effectively applied in WSNs for anomaly detection, highlighting their potential in processing and analyzing complex data generated by IoT devices. Aboelwafa et al. [47] explored the use of autoencoders for the detection of false data injection attacks in the Industrial Internet of Things (IIoT). Their results show that this method outperforms support vector machine (SVM)-based techniques in terms of attack detection and false alarm reduction while demonstrating notable efficiency in corrupted data recovery.

8.1.4. Density-Based Anomaly Detection

Density-based anomaly detection, as with algorithms like K-means and DBSCAN, is effective in grouping data based on salient features and identifying abnormal behaviors. A practical application was carried out by Garg et al. [48], where they used these algorithms to analyze logs and manually determine the specific types of attacks associated with abnormal clusters. In most other studies, this method is combined with other methods to enhance the security of IoT systems.

However, this method can be limited by its dependence on the chosen clustering characteristics and its sensitivity to the algorithm's parameters, such as the neighborhood radius in DBSCAN. Moreover, the need for manual analysis of clusters to identify specific types of attacks can make the process less efficient for large amounts of data.

8.2. Semi-Supervised Learning

Semi-supervised learning is a machine learning approach that combines elements of supervised and unsupervised learning. While supervised learning relies on labeled data for training, and supervised learning works on unlabeled data with an exploratory objective, semi-supervised learning uses both labeled and unlabeled data to train a classifier. This method aims to solve the problem of needing large amounts of labeled data for training in supervised ML, by also incorporating unlabeled data.

However, it is important to note that although semi-supervised learning seems promising in combining the advantages of both approaches, it may not always achieve the detection accuracy offered by supervised learning. Despite this limitation, there have been some successful applications of semi-supervised learning in the field of IoT security [49].

For example, Al-Jarrah et al. [43] developed a semi-supervised multilayer clustering (SMLC) approach for network intrusion detection and prevention. This method has shown its effectiveness in learning from partially labeled data while offering detection performance comparable to supervised ML.

Rathore et al. [21] also proposed a method based on an extreme learning machine (ELM) integrating semi-supervised fuzzy C-means to improve attack detection in IoT.

9. Deep Learning

Deep learning is playing an increasingly significant role in intrusion detection, particularly in complex IoT systems. Deep learning models consisting of neural networks with multiple hidden layers, enable deeper analysis and better feature extraction from data, which is well suited to identifying complex and subtle patterns of malicious activity [50].

9.1. Popular Methods and Applications

9.1.1. Deep Neural Networks (DNNs)

DNNs have demonstrated significant improvements in intrusion detection for IoT architectures by learning directly from raw data. Ahmad et al. [4] showed that using the IoT-Botnet 2020 dataset, DNNs achieved a 0.57–2.6% increase in model accuracy and a 0.23–7.98% reduction in the false alarm rate compared to other methods, confirming their superiority in an IoT network. Jin Kim et al. [51] also studied an intrusion detection system using a DNN on the KDD Cup 99 dataset, revealing high accuracy in intrusion detection with a low false alarm rate. The DNN model achieved a detection rate of 99.95% for abnormal flows, although there was a slight decrease (3.87–10.99%) in the detection of benign flows compared to other algorithms. Despite this, the DNN still achieved a score of 96.085%, outperforming other methods. These results underline the effectiveness of DNNs in intrusion detection while highlighting the need for ongoing optimization to improve benign flow detection. The advantages of this approach include high detection accuracy and adaptability to evolving attacks. However, the complexity of DNNs and the need for large volumes of data for training are seen as disadvantages.

9.1.2. Convolutional Neural Networks (CNNs)

In the IoT sector, CNNs have been used to identify malware on Android systems. Research [33] has revealed that CNNs can automatically learn features relevant to malware detection from raw data, eliminating the need for manual feature manipulation. This technique marks an advance in traditional machine learning methods, offering complete end-to-end modeling. Kim et al. [52] conducted a study on network intrusion detection using a CNN model, focusing on detecting denial-of-service (DoS) attacks by exploiting the KDD CUP 1999 and CSE-CIC-IDS2018 datasets. Their method involves transforming data features into images to train the CNN model. The results indicate that the CNN model outperforms a model based on a recurrent neural network (RNN). Chen et al. [24] developed a network intrusion detection system based on a CNN. They trained their model using both extracted features and raw network traffic, demonstrating superior accuracy compared to models based solely on extracted features. They used standard datasets such as NSL-KDD. The main advantage of their method lies in the ability of CNNs to process raw data directly without the need for extensive pre-processing, thus improving detection. However, the complexity and high computational demands of CNNs are seen as constraints.

9.1.3. Recurrent Neural Networks (RNNs)

RNNs are particularly effective for applications in threat detection, where models are highly dependent on the temporal aspect of data. Shin Park et al. explored an intrusion detection method based on LSTM, demonstrating its superiority in terms of mean square error (MSE) and mean absolute error (MAE) compared to other techniques [53]. Tang et al. [54] proposed an intrusion detection method using a deep recurrent neural network (GRU-RNN) for SDNs, achieving 89% accuracy with six raw features. This model proved effective for real-time detection without significantly impacting network performance. Kim et al. [52] presented an intrusion detection approach using LSTM-RNN on the KDD Cup 1999 dataset, highlighting the effectiveness of LSTM-RNN in terms of detection rate and false alarms. Torres et al. [55] demonstrated the effectiveness of RNNs in analyzing network traffic behavior to identify malicious activity, confirming the crucial role of RNNs in the accurate classification of network traffic. Advances in RNN architectures, such as LSTM and GRU, have dramatically improved the ability of neural networks to handle complex data sequences, particularly in areas such as intrusion detection where accuracy and consideration of temporal dependencies are crucial [56,57].

9.1.4. Generative Adversarial Networks (GANs)

In the realm of IoT, GANs prove to be a promising approach for intrusion detection. Ferdowsi et al. [58] developed a distributed GAN architecture for a fully distributed intrusion detection system (IDS) in the IoT environment, allowing each IoT device (IoTD) to monitor its own data as well as that of its neighbors. This method is particularly beneficial for maintaining data privacy. Eunbi Seo et al. [26] designed an intrusion detection system for vehicular networks using GANs, named GIDS, to identify unknown attacks based solely on normal data. Their trials showed high accuracy in detection, although distinguishing normal component failures from deliberate attacks remains a challenge. Dashun Liao et al. [59] proposed a network intrusion detection method based on GANs, focusing on enhancing attack detection by generating new training data. Their approach demonstrated significant improvement over conventional methods when tested with various datasets. Simulation results on a daily activity recognition dataset revealed that the distributed GAN proposed by Ferdowsi et al. [58] provides up to 20% additional accuracy, a 25% improvement in precision, and a 60% reduction in false positive rate compared to a standalone GAN. These results highlight the superior effectiveness of the distributed GAN solution for precise intrusion detection with less dependence on central units and better preservation of data privacy.

Tables 6 and 7 summarize all the methods discussed in the literature.

Table 6. Machine learning methods for intrusion detection in IoT.

Method	Study	Dataset	Attacks and Vulnerabilities Explored	Results
ANN	[28]	UNSW-15 Dataset	Dos, Probe, U2R, R2L	Average precision of 84%, false positive rate < 8%
	[27]	Simulated with Contiki OS/Cooja Simulator 3.0	DIS attack, Version attack	Accurate classification, low error rate
SVM	[30]	KDD Cup 99	Various types of attacks	Significant reduction in false positives
	[18]	UNSW-NB15	Backdoor, DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, Worms	85.99% precision in binary classification, 75.77% in multi-classification
KNN	[36]	DoH20	Various types of attacks	100% precision for KNN and DT
	[34,36]	University of New Mexico data	Dos, Probe, U2R, R2L	Reduced execution time up to 0.01%, decreased error rates up to 0.002%
Naive Bayes	[60]	KDD Cup'99	DoS, Probe, U2R, R2L	Improved false positive rates, cost, and calculation time
Logistic Regression	[38]	Malware Capture Facility Project, Stratosphere IPS data	Traffic from 8 different botnet families	AUC of 0.985, precision of 95%, recall of 96.7%
	[39]	CIC-IDS 2017	DDoS and Bot	73.79% precision with information gain-based feature selection
Decision Tree	[41]	NSL-KDD	DOS and DDOS attacks	73.79% precision in DDoS attack detection
	[42]	NSL-KDD	Various IoT attacks	Improved precision and model construction time

Table 7. Machine learning methods for intrusion detection in IoT.

Method	Study	Dataset	Attacks and Vulnerabilities Explored	Results
K-means	[44]	MIT-DARPA 1999 network traffic data	DDOS attacks, code injection	Improved precision, reduced false positives
K-means and PCA	[45]	KDD Cup 99	Various attacks	-
Autoencoder	[46]	Indoor WSN testbed	Various attacks	High detection accuracy, low false alert rate
	[47]	IIoT industry-specific	False data injection attacks targeting IIoT	Significant improvement in attack detection compared to SVM-based methods
DBSCAN	[48]	Not specified	Various varied attacks	Effective data clustering and identification of abnormal behavior
DNN	[4]	IoT-Botnet 2020	Various types of attacks	High precision, adaptability, detects complex patterns
	[51]	KDD Cup 99	-	-
CNN	[52]	KDD CUP 1999 and CSE-CIC-IDS2018	DoS attacks	Effective for malware detection on Android, superior to RNNs for DoS detection
	[24]	CIC-IDS	Various attacks	-
RNN	[53]	NSL-KDD	Various attacks	-
	[54]	NSL-KDD	Attacks in SDN networks	89% precision with only six raw features
GAN	[55]	Bot-IoT Dataset	Botnet behaviors in network traffic	High attack detection rate with low false alarm rate, challenges with indistinguishable and unbalanced traffic
	[58]	Daily activity recognition dataset collected from 30 subjects using a smartphone	Internal and external attacks, including false data injections	Distributed GAN shows up to 20% higher precision, 25% higher recall, and 60% lower false positive rate compared to standalone GAN
	[59]	KDD Cup 99	-	Excellent results for intrusion detection, with approximately 99% precision for all cases and high detection rate

9.2. Review of Datasets

The evolution of intrusion detection datasets illustrates changes in threats and technological advancements in the IoT domain. Through the literature review, we present the following Table 8, which summarizes the timeline of the datasets, the types of attacks they include, and the studies that used them.

Table 8. Datasets in IoT.

Dataset	Attack	Data Size	Data Type	Study
DARPA1998	Dos, Probe, U2R, R2L	Varies	Raw packets	[44]
KDD Cup 99	Dos, R2L, U2R, Probing	4,730,503 packets	Network records	[45,52,59–62]
NSL-KDD	DoS, R2L, U2R, Probe with 22 types of subcategories of attacks	149,470	Network records	[41,42,53,54]
UNSW-NB15	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms	2.5 GB	PCAP, CSV	[18,28]
CIDDS-001	Port scan, Dos, Ping of Death, etc.	700 MB	Data flows, CSV	[63–65]
CIC-IDS-2017 and CSE-CIC-IDS2018	Bot, brute force, DoS, Infiltration, SQL injection	Varies greatly	PCAP, CSV	[18,39]

Table 8. *Cont.*

Dataset	Attack	Data Size	Data Type	Study
BoT-IoT	DDoS, DoS, Reconnaissance, Theft	5 GB	PCAP, CSV	[4,55]
Edge-IIoTset	DDoS_UDP, DDoS_ICMP, SQL_injection, Password, Vulnerability_scanner, DDoS_TCP, DDoS_HTTP, Uploading, Backdoor, Port_Scanning, XSS, Ransomware, MITM, Fingerprinting	Varies also	Network traffic flows, Security event logs, IoT device metrics, Specific attack records, Web traffic data, Communication metadata	No studying

10. Discussion

As we deepen our understanding of intrusion detection systems in IoT environments, it is crucial to examine the challenges and current limitations, as well as the trends and emerging innovations shaping this rapidly evolving field.

10.1. Challenges and Current Limitations

In the field of intrusion detection for IoT systems, several major challenges need to be overcome to improve the effectiveness of detection models. The first challenge concerns the creation and updating of datasets. Currently, the lack of diversity and representativeness in datasets limits the effectiveness of intrusion detection systems (IDSs), as they struggle to reflect the complexity of IoT environments. In addition, the various models proposed in the literature are often tested on heterogeneous data, making it difficult to establish a standard comparison indicator to assess their performance. Given these limitations, it is essential to develop datasets specifically adapted to IoT networks, taking into account their unique characteristics and specific threats. Constant updating and evolution of these datasets are also necessary to keep pace with current trends in cybersecurity attacks, which implies the integration of more sophisticated and diversified attack scenarios. It is also crucial to achieve adequate data balance and representativeness. This means ensuring a balanced distribution between different types of attack and normal traffic, to enhance the reliability of IDSs. Careful selection of features is also very important for optimizing models for intrusion detection and making them less complex. Optimizing hyperparameters in hybrid models is another obstacle. The complexity of these architectures makes their calibration difficult, directly affecting the reliability of IDSs, especially in resource-constrained environments. The generalization of IDS models to real-life scenarios remains a major challenge. Indeed, the performances obtained on laboratory datasets do not necessarily translate into real-world environments. This situation underlines the need to adapt and test models under conditions more representative of the real world. Finally, IDS models in IoT systems face significant resource constraints. The limited computing and storage capacity of IoT devices restricts the implementation of complex and sophisticated models, directly impacting the sophistication and effectiveness of detection methods.

10.2. Current Trends

Current trends in intrusion detection in IoT systems are marked by rapid evolution due to advances in technologies and methods. The adoption of advanced artificial intelligence techniques, such as deep and unsupervised learning, is radically transforming the ability of intrusion detection systems (IDSs) to analyze and understand data. These techniques enable more accurate and rapid identification of anomalies, which are essential for the security of IoT networks. New perspectives arise from the integration of federated learning and reinforcement learning. These innovative techniques contribute to the development of more privacy-friendly and adaptive IDS models, responding to the growing complexity of security threats in IoT environments. Class balancing and feature selection have become unquestionable milestones. In addition, optimizing the hyperparameters of IDS models

is now a priority. Such precision in model tuning is essential for adapting to the specific challenges of IoT environments. Finally, there is a growing trend toward real-time detection and the creation of fast, reactive models. An essential element of proactive security for IoT systems is the acceleration of intrusion detection and response through parallel processing and edge computing. These trends illustrate the crucial importance of continuous innovation and cross-industry collaboration in IoT security. They highlight the need for advanced, tailored solutions to overcome current and future challenges, particularly in terms of data protection and compliance with security standards. In applying machine learning models to IoT environments, several unique challenges and requirements must be addressed. The application of machine learning models in IoT environments presents unique challenges and requirements, particularly concerning resource constraints, real-time processing needs, and the diversity of IoT devices. A comparative analysis of different models highlights their strengths and weaknesses with respect to IoT-specific metrics such as energy efficiency, processing time, and adaptability to various types of IoT attacks. Support vector machines (SVMs) offer high accuracy in detecting intrusions and are robust against overfitting with proper kernel selection, but they come with high computational costs and memory usage, and are sensitive to parameter tuning, making them less effective with dynamic IoT data. Decision trees are easy to interpret, have fast training and prediction times, and are effective in feature selection, but they are prone to overfitting and less effective in handling complex and varied IoT data. K-nearest neighbors (KNNs) are simple to implement and effective in detecting anomalies, yet they have high computational costs for large datasets, are sensitive to the choice of 'k', and are impacted by noisy data. Deep neural networks (DNNs) provide high accuracy, are capable of learning complex patterns from raw data, and are adaptable to various types of attacks, but they require large datasets for training, are computationally intensive, and have the potential for overfitting without proper regularization. Autoencoders are effective in anomaly detection, reduce the dimensionality of data, and can handle unsupervised learning, but they may lose important information during compression and are less effective in highly noisy environments. Generative adversarial networks (GANs) can generate synthetic data for training, are effective in detecting unknown attacks, and preserve data privacy, but they have high computational costs, training instability, and require careful balancing of the generator and discriminator. Recurrent neural networks (RNNs) capture temporal dependencies in data and are effective in sequential data analysis, but they are prone to the vanishing gradient problem, have high computational and memory requirements, and are less effective for non-sequential data. To effectively evaluate the performance of machine learning models in IoT environments, it is important to consider IoT-specific metrics. Energy efficiency is critical due to the limited power resources of IoT devices. The processing time is crucial for real-time applications. Adaptability is key for the model's capability to adapt to various types of IoT attacks and different IoT device characteristics. Scalability measures the model's performance as the number of IoT devices and data volume increases. Finally, accuracy, including precision and recall in detecting true positives and minimizing false positives, ensures the chosen machine learning models can effectively enhance the security of IoT systems while meeting their unique constraints and requirements.

11. Conclusions

This literature review highlights the crucial importance of security in the rapidly expanding domain of the Internet of Things (IoT). Through an in-depth analysis, we have explored the inherent challenges in IoT system security, highlighting the vulnerabilities and types of attacks that threaten the stability and reliability of these technologies.

Our study has emphasized the evolution of intrusion detection systems, focusing on the limitations of traditional methods. In this context, machine learning emerges as a promising solution, capable of adapting and responding to the complex and constantly evolving threats in the IoT environment. The review has examined in detail various machine learning approaches, including supervised, unsupervised, and deep learning, evaluating their effectiveness in intrusion detection.

Nevertheless, despite significant advancements, there remain challenges and opportunities for improvement. The effectiveness of models must be evaluated within real-world scenarios, and their large-scale deployment demands careful attention to practical aspects.

Looking forward, this review encourages continued research in the field of intrusion detection for IoT, emphasizing the development of innovative solutions. It is imperative to continue exploring approaches that not only detect intrusions effectively but are also viable within the dynamic and heterogeneous framework of IoT.

Author Contributions: Conceptualization, B.R.K. and M.A.; methodology, B.R.K. and M.A.; validation, B.R.K. and M.A.; formal analysis, B.R.K.; investigation, B.R.K.; resources, B.R.K.; data curation, B.R.K. and M.A.; writing—original draft preparation, B.R.K.; writing—review and editing, B.R.K.; visualization, B.R.K. and M.A.; supervision, M.A.; project administration, B.R.K. and M.A.; funding acquisition, B.R.K. and M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ashton, K. That 'Internet Of Things' Thing. *RFID J.* **2009**, *2*, 97–114.
2. Perera, C.; Liu, C.H.; Jayawardena, S.; Chen, M. A Survey on Internet of Things From Industrial Market Perspective. *IEEE Access* **2014**, *2*, 1660–1679. [CrossRef]
3. Islam, N.; Farhin, F.; Sultana, I.; Kaiser, M.S.; Rahman, M.S.; Mahmud, M.; Hosen, A.S.M.S.; Cho, G.H. Towards Machine Learning Based Intrusion Detection in IoT Networks. *Comput. Mater. Contin.* **2021**, *69*, 1801–1821. [CrossRef]
4. Ahmad, Z.; Khan, A.S.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.R.; Tarmizi, S.; Rodrigues, J.J.P.C. Anomaly Detection Using Deep Neural Network for IoT Architecture. *Appl. Sci.* **2021**, *11*, 7050. [CrossRef]
5. Union Internationale des Télécommunications. *Infrastructure Mondiale de l'Information, Protocole Internet et RÉSeaux de Prochaine Génération*; UIT: Tromsø, Norway, 2012.
6. Corici, A.A.; Emmelmann, M.; Luo, J.; Shrestha, R.; Corici, M.; Magedanz, T. IoT inter-security domain trust transfer and service dispatch solution. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 694–699. [CrossRef]
7. Sha, K.; Errabelly, R.; Wei, W.; Yang, T.A.; Wang, Z. EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security. In Proceedings of the 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), Madrid, Spain, 14–15 May 2017; pp. 81–88. [CrossRef]
8. Al-Sarawi, S.; Anbar, M.; Abdullah, R.; Al Hawari, A.B. Internet of Things Market Analysis Forecasts, 2020–2030. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 449–453. [CrossRef]
9. Görmüş, S.; Aydın, H.; Ulutaş, G. Security for the internet of things: A survey of existing mechanisms, protocols and open research issues. *J. Fac. Eng. Archit. Gazi Univ.* **2018**, *33*, 1247–1272.
10. Ibrahim, M.; Abdullah, M.T.; Abdullah, A.; Perumal, T. An Epidemic Based Model for the Predictions of OOFI in an IoT Platform. *Int. J. Eng. Trends Technol.* **2020**, 52–56. [CrossRef]
11. Rebah, H.B. Gateway IoT de pilotage et de surveillance des capteurs domestiques via le protocole MQTT. *Researche Gate* **2022**, *3*.
12. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
13. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* **2021**, *12*, 87. [CrossRef]
14. Hasan, M.A.M.; Nasser, M.; Ahmad, S.; Molla, K.I. Feature Selection for Intrusion Detection Using Random Forest. *J. Inf. Secur.* **2016**, *7*, 129–140. [CrossRef]
15. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Emeishan, China, 14–15 December 2013; pp. 663–667. [CrossRef]
16. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
17. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
18. Jing, D.; Chen, H.B. SVM Based Network Intrusion Detection for the UNSW-NB15 Dataset. In Proceedings of the 2019 IEEE 13th International Conference on ASIC (ASICON), Chongqing, China, 29 October–1 November 2019; pp. 1–4. [CrossRef]
19. Weber, R.H.; Studer, E. Cybersecurity in the Internet of Things: Legal aspects. *Comput. Law Secur. Rev.* **2016**, *32*, 715–728. [CrossRef]

20. Chen, Z.; Liu, J.; Shen, Y.; Simsek, M.; Kantarci, B.; Mouftah, H.T.; Djukic, P. Machine Learning-Enabled IoT Security: Open Issues and Challenges under Advanced Persistent Threats. *ACM Comput. Surv.* **2023**, *55*, 1–37. [CrossRef]
21. Rathore, S.; Park, J.H. Semi-supervised learning based distributed attack detection framework for IoT. *Appl. Soft Comput.* **2018**, *72*, 79–89. [CrossRef]
22. Mishra, A.K.; Tripathy, A.K.; Puthal, D.; Yang, L.T. Analytical Model for Sybil Attack Phases in Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 379–387. [CrossRef]
23. Chen, B.; Ho, D.W.C.; Hu, G.; Yu, L. Secure Fusion Estimation for Bandwidth Constrained Cyber-Physical Systems under Replay Attacks. *IEEE Trans. Cybern.* **2018**, *48*, 1862–1876. [CrossRef]
24. Chen, L.; Kuang, X.; Xu, A.; Suo, S.; Yang, Y. A Novel Network Intrusion Detection System Based on CNN. In Proceedings of the 2020 Eighth International Conference on Advanced Cloud and Big Data (CBD), Taiyuan, China, 5–6 December 2020; pp. 243–247. [CrossRef]
25. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Appl. Sci.* **2019**, *9*, 4396. [CrossRef]
26. Sundararajan, K.; Garg, L.; Srinivasan, K.; Bashir, A.K.; Kaliappan, J.; Ganapathy, G.P.; Selvaraj, S.K.; Meena, T. A Contemporary Review on Drought Modeling Using Machine Learning Approaches. *Comput. Model. Eng. Sci.* **2021**, *128*, 447–487. [CrossRef]
27. Anitha, A.A.; Arockiam, D.L. ANNIDS: Artificial Neural Network based Intrusion Detection System for Internet of Things. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 2583–2588. [CrossRef]
28. Hanif, S.; Ilyas, T.; Zeeshan, M. Intrusion Detection In IoT Using Artificial Neural Networks On UNSW-15 Dataset. In Proceedings of the 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Charlotte, NC, USA, 6–9 October 2019; pp. 152–156. [CrossRef]
29. Jamal, A.; Faisal, H.M.; Nasir, M. Malware Detection and Classification in IoT Network using ANN. *Mehran Univ. Res. J. Eng. Technol.* **2022**, *41*, 80–91. [CrossRef]
30. Goeschel, K. Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp. 1–6. [CrossRef]
31. Ioannou, C.; Vassiliou, V. Network Attack Classification in IoT Using Support Vector Machines. *J. Sens. Actuator Netw.* **2021**, *10*, 58. [CrossRef]
32. Pouyanfar, S.; Sadiq, S.; Yan, Y.; Tian, H.; Tao, Y.; Reyes, M.P.; Shyu, M.L.; Chen, S.C.; Iyengar, S.S. A Survey on Deep Learning. *ACM Comput. Surv.* **2019**, *51*, 1–36. [CrossRef]
33. Zhu, R.; Ji, X.; Yu, D.; Tan, Z.; Zhao, L.; Li, J.; Xia, X. KNN-Based Approximate Outlier Detection Algorithm over IoT Streaming Data. *IEEE Access* **2020**, *8*, 42749–42759. [CrossRef]
34. Abdaljabar, Z.H.; Ucan, O.N.; Alheeti, K.M.A. An Intrusion Detection System for IoT Using KNN and Decision-Tree Based Classification. In Proceedings of the 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI), Sana'a, Yemen, 4–6 December 2021; pp. 1–5. [CrossRef]
35. Li, W.; Yi, P.; Wu, Y.; Pan, L.; Li, J. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network. *J. Electr. Comput. Eng.* **2014**, *2014*, 1–8. [CrossRef]
36. Govindarajan, M.; Chandrasekaran, R. Intrusion detection using k-Nearest Neighbor. In Proceedings of the 2009 First International Conference on Advanced Computing, Chennai, India, 13–15 December 2009; pp. 13–20. [CrossRef]
37. Aref, M.A.; Jayaweera, S.K.; Machuzak, S. Multi-Agent Reinforcement Learning Based Cognitive Anti-Jamming. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6. [CrossRef]
38. Bapat, R.; Mandya, A.; Liu, X.; Abraham, B.; Brown, D.E.; Kang, H.; Veeraraghavan, M. Identifying malicious botnet traffic using logistic regression. In Proceedings of the 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 27–27 April 2018; pp. 266–271. [CrossRef]
39. Sambangi, S.; Gondi, L. A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. *Proceedings* **2020**, *63*, 51. [CrossRef]
40. Qaddoura, R.; Al-Zoubi, A.M.; Almomani, I.; Faris, H. A Multi-Stage Classification Approach for IoT Intrusion Detection Based on Clustering with Oversampling. *Appl. Sci.* **2021**, *11*, 3022. [CrossRef]
41. Ingre, B.; Yadav, A.; Soni, A.K. *Decision Tree Based Intrusion Detection System for NSL-KDD Dataset*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 207–218. [CrossRef]
42. Rai, K.; Devi, M.S.; Guleria, A. Decision Tree Based Algorithm for Intrusion Detection. *Adv. Netw. Appl.* **2016**, *7*, 2828–2834.
43. Al-Jarrah, O.Y.; Al-Hammdi, Y.; Yoo, P.D.; Muhaidat, S.; Al-Qutayri, M. Semi-supervised multi-layered clustering model for intrusion detection. *Digit. Commun. Netw.* **2018**, *4*, 277–286. [CrossRef]
44. Muniyandi, A.P.; Rajeswari, R.; Rajaram, R. Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree Algorithm. *Procedia Eng.* **2012**, *30*, 174–182. [CrossRef]
45. Peng, K.; Leung, V.C.M.; Huang, Q. Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System over Big Data. *IEEE Access* **2018**, *6*, 11897–11906. [CrossRef]
46. Luo, T.; Nagarajan, S.G. Distributed Anomaly Detection Using Autoencoder Neural Networks in WSN for IoT. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [CrossRef]

47. Aboelwafa, M.M.N.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. *IEEE Internet Things J.* **2020**, *7*, 8462–8471. [CrossRef]
48. Garg, S.; Kaur, K.; Batra, S.; Kaddoum, G.; Kumar, N.; Boukerche, A. A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. *Future Gener. Comput. Syst.* **2020**, *104*, 105–118. [CrossRef]
49. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
50. Brun, O.; Yin, Y.; Yin, Y.; Gelenbe, E. Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-Connected Home Environments. In *Security in Computer and Information Sciences: First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26–27 2018, Revised Selected Papers 1*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 458–463.
51. Kim, J.; Shin, N.; Jo, S.Y.; Kim, S.H. Method of intrusion detection using deep neural network. In Proceedings of the 2017 IEEE International Conference on Big Data and Smart Computing (BigComp), Jeju, Republic of Korea, 13–16 February 2017; pp. 313–316. [CrossRef]
52. Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics* **2020**, *9*, 916. [CrossRef]
53. Park, S.H.; Park, H.J.; Choi, Y.J. RNN-Based Prediction for Network Intrusion Detection. In Proceedings of the 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 19–21 February 2020; pp. 572–574. [CrossRef]
54. Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M. Deep Recurrent Neural Network for Intrusion Detection in SDN-Based Networks. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 202–206. [CrossRef]
55. Torres, P.; Catania, C.; Garcia, S.; Garino, C.G. An analysis of Recurrent Neural Networks for Botnet detection behavior. In Proceedings of the 2016 IEEE Biennial Congress of Argentina (ARGENCON), Buenos Aires, Argentina, 15–17 June 2016; pp. 1–6. [CrossRef]
56. Hochreiter, S.; Schmidhuber, J. Long Short-Term Memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef] [PubMed]
57. Chung, J.; Gulcehre, C.; Cho, K.; Bengio, Y. Evaluation of gated recurrent neural networks on sequence modeling. *arXiv* **2014**, arXiv:1412.3555.
58. Ferdowsi, A.; Saad, W. Generative Adversarial Networks for Distributed Intrusion Detection in the Internet of Things. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]
59. Liao, D.; Huang, S.; Tan, Y.; Bai, G. Network Intrusion Detection Method Based on GAN Model. In Proceedings of the 2020 International Conference on Computer Communication and Network Security (CCNS), Xi'an, China, 21–23 August 2020; pp. 153–156. [CrossRef]
60. Panda, M.; Patra, M.R. Network Intrusion Detection Using Naïve Bayes. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2007**, *7*, 258–263.
61. Gumus, F.; Sakar, C.O.; Kursun, O. Network Intrusion Detection Using Naïve Bayes. In Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Beijing, China, 17–20 August 2014.
62. Kim, J.; Kim, J.; Thu, H.L.T.; Kim, H. Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection. In Proceedings of the 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Republic of Korea, 15–17 February 2016; pp. 1–5. [CrossRef]
63. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
64. Cassales, G.W.; Senger, H.; de Faria, E.R.; Bifet, A. IDSA-IoT: An Intrusion Detection System Architecture for IoT Networks. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; pp. 1–7.
65. Yahyaoui, A.; Lakhdhar, H.; Abdellatif, T.; Attia, R. Machine learning based network intrusion detection for data streaming IoT applications. In Proceedings of the 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter), Ho Chi Minh City, Vietnam, 28–30 January 2021; pp. 51–56. [CrossRef]

CHAPITRE 2APPRENTISSAGE AUTOMATIQUE POUR LA DETECTION DES ATTAQUES DOS DANS LES SYSTEMES IOT : APPROCHE METHODOLOGIQUE, RESULTATS ET ANALYSE

2.1 RESUMÉ EN FRANÇAIS DE L'ARTICLE 02: MACHINE LEARNING FOR DOS ATTACK DETECTION IN IOT SYSTEMS[14]

Cet article présente une étude approfondie sur le développement d'un modèle d'apprentissage pour la détection des attaques DoS dans les systèmes IoT. L'objectif principal de cette recherche est d'améliorer la précision et l'efficacité de la détection en exploitant des techniques avancées d'équilibrage de classes et de sélection de fonctionnalités. Nous avons utilisé un ensemble de données Edge IIoT et appliqué SMOTE et Random Undersampling pour équilibrer les classes, tandis que DNN, Random Forest et PCA ont été utilisés pour sélectionner les fonctionnalités les plus pertinentes.

Notre méthodologie comprend l'évaluation de six combinaisons de ces techniques avec quatre classificateurs optimisés (DNN, SVM, XGBoost et Random Forest) pour identifier la stratégie la plus efficace. Les résultats montrent que certaines combinaisons offrent une amélioration significative des performances de détection par rapport aux approches traditionnelles. L'optimisation des classificateurs à l'aide de techniques telles que Grid Search pour SVM, Keras Tuner pour DNN et Optuna pour XGBoost a permis d'obtenir un équilibre optimal entre précision et vitesse de classification.

En conclusion, cette recherche fournit une méthodologie robuste pour la détection des attaques DoS dans les systèmes IoT, offrant ainsi une contribution significative à la sécurité des infrastructures IoT. Les résultats de cette étude ouvrent la voie à de futures recherches visant à renforcer la détection des menaces de sécurité dans les systèmes IoT. Cet article est accepté et sera présenté lors de la conférence international MobiSPC qui aura lieu en Aout 2024.

2.2 MACHINE LEARNING FOR DOS ATTACK DETECTION IN IOT SYSTEMS[14]

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2019) 000–000
www.elsevier.com/locate/procedia

Procedia Computer Science

The 21st International Conference on Mobile Systems and Pervasive Computing (MobiSPC)
August 5-7, 2024, Marshall University, Huntington, WV, USA

Machine Learning for DoS Attack Detection in IoT Systems

Brunel Rolack KIKISSAGBE[a], Mehdi Adda[a], Paul Célicourt[b], Igor TCHAPPI HAMAN[c], Amro Najjar[c]

[a]Mathematics, Computer Science, and Engineering Departement. University of Quebec at Rimouski, Canada (QC) [b]National Institute of Scientific Research, Canada (QC) [c]University of Luxembourg, Luxembourg

Abstract

This study focuses on enhancing DoS attack detection in IoT systems through a Machine Learning approach that combines class balancing, feature selection, and optimized classifiers. Utilizing the Edge IIoT dataset, we applied SMOTE and Random Undersampling for class balance and employed DNN, Random Forest, and PCA for feature selection. We evaluated six technique combinations across four classifiers (DNN, SVM, XGBoost, and Random Forest), finding that certain combinations notably improve detection efficiency and accuracy. This research contributes to IoT security by offering an effective methodology for DoS attack detection, setting a foundation for further advances in IoT system protection against security threats.

Keywords: IoT; Security; Intrusion Detection; Machine Learning,; DoS

INTRODUCTION

Initiated by Kevin Ashton [1], the Internet of Things (IoT) has transformed how we interact with the world around us [2]. IoT's rapid growth has escalated security vulnerabilities, particularly the threat of Denial of Service (DoS) and Distributed Denial of Service (DDoS)

attacks [3, 4]. These attacks, characterized by their ability to inundate networks with traffic, pose a critical risk to essential services and infrastructure. In this context, developing effective intrusion detection methods has become essential to protect IoT infrastructures. Traditional methods are often ill-suited to the specificities of the IoT, such as the diversity of devices and protocols, as well as their processing and

* Corresponding author. Tel. : +0-000-000-0000; fax : +0-000-000-0000. *E-mail address:* Brunel.Kikissagbe@uqar.ca

storage constraints[5]. Machine learning (ML) is a promising approach for developing dynamic systems that effectively counter DoS and DDoS attacks. Although numerous studies have explored intrusion detection in IoT systems using machine learning [6], there is still a need to improve the accuracy and efficiency of detection models in the face of DoS attacks. Consequently, this study explores the application of several ML techniques to enhance the detection of DoS attacks within IoT systems, aiming to surmount the limitations of existing methods.

The research question guiding this study is : How can we improve the detection of DoS attacks in IoT systems using Machine Learning models? This investigation proposes an approach that combines various ML techniques—including class balancing (SMOTE, Random Undersampling), feature selection (DNN, Random Forest, PCA), and classification (SVM, DNN, XGBoost, Random Forest)—to construct effective models for identifying DoS activities.

The structure of this paper is organized as follows : Section 2 reviews related work in the field. Section 3 outlines our methodology, including data handling and model selection procedures. Following the methodology, Section 4 presents experiments conducted according to the described methods. Section 5 then presents the results of evaluating the

performance of these models, and Section 6 discusses the implications of the findings. Finally, the paper concludes in Section 7, summarizing the key contributions and suggesting avenues for future research.

RELATED WORK

Detecting DoS attacks in IoT systems has attracted growing interest in research, where various ML methods have been explored for their effectiveness. For example, Artificial Neural Networks (ANNs) were successfully applied in the study [7] using the UNSW-15 Dataset for attacks such as DoS and Probe, achieving an average accuracy of 84%. Another study by [8] also reported good results in a similar context. However, this study highlighted the need for improved optimizers and activation and loss functions to boost performance.

Similarly, the Support Vector Machine (SVM) method has been used in various studies, such as [9] [10] on the KDD Cup 99 dataset, revealing a significant reduction in false positives. Nevertheless, it highlights a need to improve processing flexibility and efficiency for diversified IoT data[9].

On the other hand, other methods such as K-Nearest Neighbors (KNN) and Naives (NB) Bayes have shown high accuracy in detecting attacks but have also revealed limitations in terms of execution time and dealing with the impact of noise [11]. Decision tree-based techniques, such as the study [12] [13] on the NSL-KDD dataset, showed promising accuracy in detecting DDoS attacks, but highlighted the need for better feature selection.

In addition, Logistic Regression was applied in [14] and [15] to detect botnet traffic of different families and DDoS and Bot attacks, respectively, obtaining promising results in terms of precision, recall, and AUC.

Decision Tree was used in [12] and [13] to detect DoS and DDoS attacks on the NSL-KDD dataset, showing an accuracy of 73.79% in the detection of DDoS attacks and an improvement in accuracy and model building time. Random Forest has been successfully applied in various intrusion detection studies [12] [13], demonstrating its effectiveness in accurately classifying complex attacks while handling large dimensions of datasets

Kmeans was used in [16] and combined with PCA in [17] to detect various attacks on the KDD Cup 99 and MIT-DARPA 1999 network traffic datasets, showing improved accuracy and reduced false positives.

More recent approaches, such as Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN), have been explored for their ability to detect complex patterns and adapt to evolving threats [18]. For example, DNNs were explored in [4] and [19] to detect various types of attack on the IoT-Botnet 2020 and KDD Cup 99 datasets, offering high accuracy and adaptability to complex patterns. Recurrent neural networks (RNN) have demonstrated their effectiveness in intrusion detection, achieving 89% accuracy with only six raw features in SDN networks (NSL-KDD dataset) [20] and adapting to various attacks, including DoS, R2L, U2R and Probe (KDD Cup 1999 dataset) [21]. However, these methods highlighted challenges regarding architecture complexity and computational requirements [22].

Finally, Generative Adversarial Networks (GANs) have been used to detect botnet behavior with high attack detection rates, but have encountered difficulties with poorly differentiable and unbalanced traffic [23] [24]

By testing different combinations of techniques, we aim to determine the most effective strategy for detecting DoS and DDoS attacks.

METHODOLOGY

For class balancing, we utilized the Synthetic Minority Over-sampling Technique (SMOTE) and Random Undersampling to address class imbalances, enhancing the model's ability to identify DoS attacks accurately.

In this study, we employed a structured methodology to enhance the detection of Denial of Service (DoS) attacks within Internet of Things (IoT) systems through ML techniques. Our approach began with the selection and preprocessing of the Edge IIoT Dataset, which included encoding categorical features, removing irrelevant data points, and normalizing the dataset to ensure uniformity in feature contribution. Given the dataset's diverse array of attack types and extensive volume of network traffic records, it was essential to apply class balancing and feature selection techniques to address its complexity and variability effectively. For class balancing, Synthetic Minority Over-sampling Technique (SMOTE)[25] and Random Undersampling (RUS)[26] were employed to mitigate issues stemming from class imbalance.

Feature selection is beneficial for improving model performance. The presence of irrelevant or redundant features can dilute useful information and hinder the model's ability to effectively distinguish between normal activities and attacks [27]. To isolate the most significant features for attack detection, Deep Neural Networks (DNN)[28], Random Forest[29], and Principal Component Analysis (PCA)[30] were utilized for feature selection. The classification stage integrated four distinct models : Support Vector Machine (SVM), Deep Neural Network (DNN), XGBoost, and Random Forest (RF), each fine-tuned through specific hyperparameter optimization techniques.

Exploring the impact of each technique on model performance is essential to determine the most appropriate combination for our specific case. Thus, different combination of techniques (Feature Selection, Balancing dataset, Classification) are tested (c.f. Section 4) and results are reported (c.f. Section 5). These models underwent comprehensive evaluation, employing metrics like precision, recall, F1-score, and accuracy, in conjunction

with analytical tools including confusion matrices, ROC curves, and stratified cross-validation to ascertain their effectiveness in detecting DoS attacks. The methodology outlined here, illustrated in Fig. 1, reflects our systematic approach to identifying an optimal ML model for bolstering the security of IoT systems against DoS attacks.

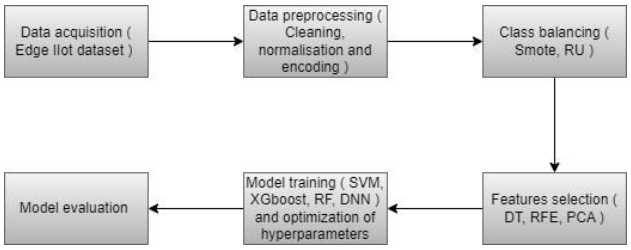

Figure 1. Summary of Methodology

EXPERIMENTS

Following the methodology described in Section 3, we conducted a set of experiments whose main informationare described below.

Encoding Categorical Features :. Several features in our dataset are categorical, such as "http.request.method", "http.referer", "http.request.version", "mqtt.protoname", "mqtt.topic", and "dns.qry.name.len". We used encoding techniques, such as one-hot encoding, to transform these features into a numerical format so that they could be processed by our machine learning model.

Removing Irrelevant Data :. Some columns in the dataset, such as "frame.time", "ip.src_host", "ip.dst_host", and others, were identified as irrelevant for DoS attack detection. Furthermore, we removed duplicate rows, missing values (NaN), and null entries to ensure data integrity.

Normalizing Data :. We normalized the dataset to ensure that all features contribute equally to the model's learning. This step is crucial to prevent features with larger value ranges from dominating those with smaller ranges.

Grouping Attacks :. In line with our classification goal, we grouped different DoS attacks under a single category by assigning 1 to the "Attack_group" column for instances corresponding to DoS attacks and 0 for other activities, including other types of attacks and normal traffic. After grouping, we had 1,638,533 instances for DoS attacks and 1,288,771 instances for other types. The heterogeneous class distribution highlights the importance of applying class balancing techniques, to avoid biases in attack detection.

These preprocessing steps transformed the Edge IIoT dataset into a format suitable for binary classification of DoS attacks.

2.3 CLASS BALANCING AND FEATURE SELECTION

Fig. 2 shows a heterogeneous class distribution. To help avoid biased results and ensure a fair representation of all classes, two class balancing methods, SMOTE and RUS, are examined to determine which is most appropriate for our context.

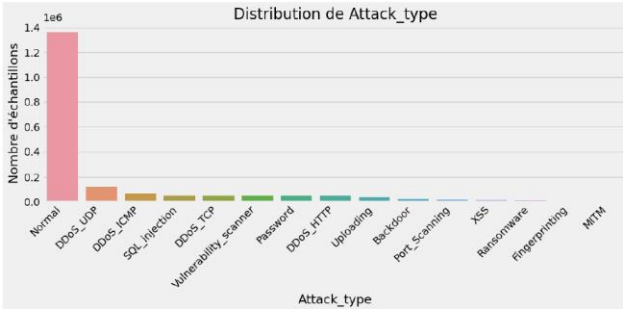

Figure 2. Attack type distribution

The Edge IIoT dataset initially has 63 features, including information on communication protocols, IP addresses, ports, TCP flags, among others. Faced with such diversity and quantity of variables, it becomes imperative to identify those that are truly informative for DoS attack detection.

We tested three feature selection techniques to select the most important features in our dataset.

2.4 Classification Models and Optimization for Intrusion Detection

Four classification techniques are used in our experiments : Support Vector Machine (SVM), Deep Neural Network (DNN), XGBoost, and Random Forest. These techniques have been applied to each of the six combinations seen previously, resulting in 24 combinations to evaluate and compare.

In our experiments, the best hyperparameters for the SVM model are : ('C' : '10', 'gamma' : '0.0001', 'kernel' : 'rbf', 'penalty' : 'l2', 'loss' : 'hinge'). For XGBoost, the best hyperparameters are :('n_estimators' : '150', 'max_degree' : '5', 'learning rate' : '0.05', 'subsample' : '0.8', 'colsample_bytree' : '0.7') For the neural network, the hyperparameters are : ('units' : 128, 'activation function' : 'relu', 'dropout' : 0.3 , 'learning rate' : 0.001, 'optimizer' : 'adam' , 'loss function' : 'Binary Crossentropy') For the random forest, the hyperparameters are :('bootstrap' : 'true', 'max_depth' : '10', 'min_sample_leaf' : '4', 'min_samples_split' : '10' 'n_estimators' : '400')

To assess the effectiveness of our classification models in detecting DoS attacks in IoT systems, we use several evaluation metrics to provide crucial information about the model's performance : Precision, Recall, F1-Score, and Accuracy [5] .

Although we have balanced the classes in our data, we used stratified cross-validation with k=5 to evaluate our models. This approach ensures that the distribution of classes remains constant in each fold.

RESULTS

In this section, we present the performance of our classification models for detecting DoS attacks in IoT systems. The results of 24 tests are summarized in Table 1, which shows the Accuracy, Precision, Recall, and F1 score for each dataset and model combination. Using SMOTE for class balancing, Random Forest for feature selection, and SVM for classification, the results show an accuracy of 0.9502, a precision of 0.7593, a recall of 0.9794, and an F1 score of 0.8554. The combination of SMOTE, Random Forest, and

XGBoost yields improved performance, with an accuracy of 0.9834, a precision of 0.9074, a recall of 0.9909, and an F1 score of 0.9473. The use of SMOTE, Random Forest, and a neural network leads to similar results, with an accuracy of 0.9819, a precision of 0.9122, a recall of 0.9735, and an F1 score of 0.9419. The combination of Random Undersampling, a neural network, and Random Forest yields an accuracy of 0.9847, a precision of 0.9174, a recall of 0.9874, and an F1 score of 0.9511. The SMOTE + DNN combination with neural network classification achieved better results, with a precision of 0.9962, a recall of 0.9828, and an F1 score of 0.9559.

Class Balancing	Feature Selection	Model	Accuracy	Precision	Recall	F1-Score
SMOTE	RF	SVM	0.9502	0.7593	0.9794	0.8554
SMOTE	RF	XGBoost	0.9834	0.9074	0.9909	0.9473
SMOTE	RF	Neural Network	0.9819	0.9122	0.9735	0.9419
SMOTE	RF	Random Forest	0.9774	0.8786	0.9856	0.9290
RU	RF	SVM	0.9429	0.7308	0.9817	0.8379
RU	RF	XGBoost	0.9848	0.9144	0.9916	0.9515
RU	RF	Neural Network	0.9766	0.8747	0.9859	0.9270
RU	RF	Random Forest	0.9623	0.8942	0.9456	0.9236
SMOTE	PCA	SVM	0.9605	0.8028	0.9774	0.8816
SMOTE	PCA	XGBoost	0.9798	0.8884	0.9897	0.9363
SMOTE	PCA	Neural Network	0.9726	0.8525	0.9892	0.9158
SMOTE	PCA	Random Forest	0.9708	0.9217	0.8808	0.9008
RU	PCA	SVM	0.9399	0.7261	0.9644	0.8285
RU	PCA	XGBoost	0.9803	0.8918	0.9888	0.9378

RU	PCA	Neural Network	0.9815	0.8980	0.9891	0.9414
RU	PCA	Random Forest	0.9723	0.8849	0.9376	0.9105
SMOTE	DNN	SVM	0.9860	0.9220	0.9905	0.9550
SMOTE	DNN	XGBoost	0.9833	0.9361	0.9915	0.9469
SMOTE	DNN	Neural Network	0.9962	0.9828	0.9913	0.9559
SMOTE	DNN	Random Forest	0.9870	0.9352	0.9816	0.9578
RU	DNN	SVM	0.9859	0.9218	0.9905	0.9549
RU	DNN	XGBoost	0.9861	0.9230	0.9904	0.9555
RU	DNN	Neural Network	0.9861	0.9226	0.9905	0.9554
RU	DNN	Random Forest	0.9847	0.9174	0.9874	0.9511

Table 1. Classification model evaluation results.

For a visual analysis of performance, we present comparison charts for each metric (accuracy, precision, recall, Score F1) in Figures 3, 4, 5, and 6.

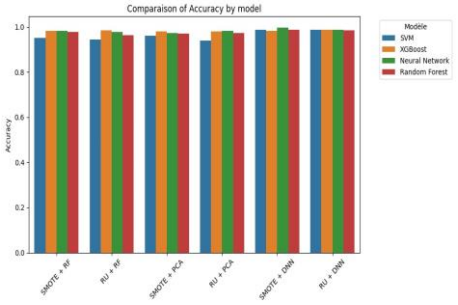

Figure 3. Comparison of Accuracy by model

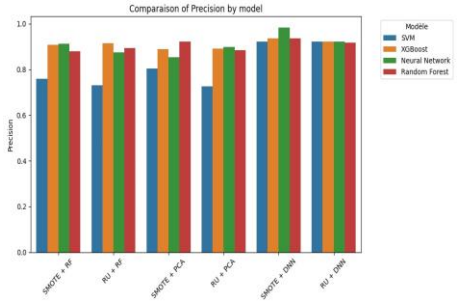

Figure 4. Comparison of Precision by model

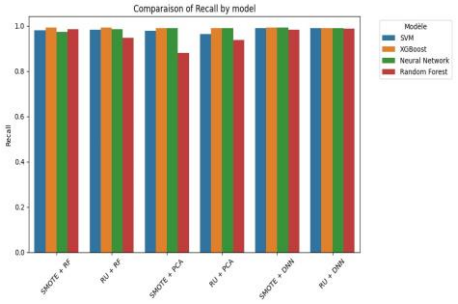

Figure 5. Comparison of Recall by model

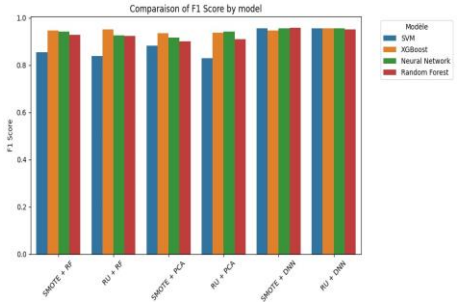

Figure 6. Comparison of F1-score by model

DISCUSSION

Our study explored the effectiveness of various classification models and combinations of feature selection and class balancing techniques for detecting DoS attacks in IoT systems. The results offer valuable insights into the most effective approaches.

The XGBoost and Neural Network models demonstrated remarkably high performance among the classifiers tested. mance on several datasets. In particular, in combination with Neural Network and SMOTE, Neural Network achieved a precision of 0.9828, recall of 0.9913, and F1 score of 0.9559. XGBoost also displayed excellent performance, especially with the combination of SMOTE and Random Forest, where it achieved an accuracy of 0.9074, a recall of 0.9909 and an F1 score of 0.9473. These results suggest that XGBoost and neural networks are particularly suitable for detecting DoS attacks in contexts where classes are unbalanced but have been previously balanced by techniques like SMOTE..

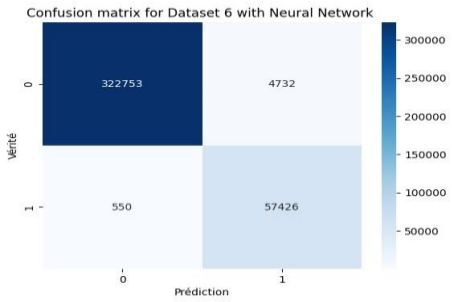

Figure 7. Confudion matrix for Smote + DNN + Neural Network

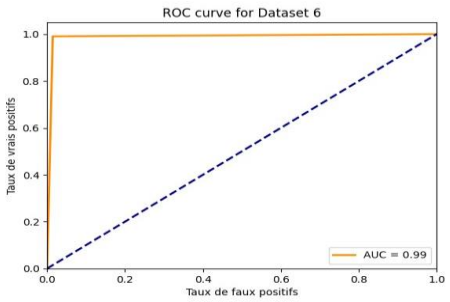

Figure 8. ROC Curve for Smote + DNN + Neural Network

The analysis of the results also reveals the importance of feature selection and class balancing. Combinations involving SMOTE tend to show better performance, highlighting

the effectiveness of this technique in addressing class imbalance. Similarly, using Random Forest for feature selection has shown promising results, indicating that this method can help identify the most relevant features for attack detection.

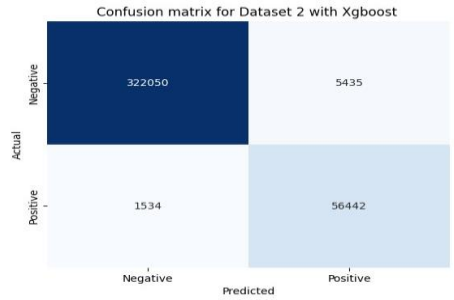

Figure 9. Confusion matrix for Smote + Random Forest + Xg-boost

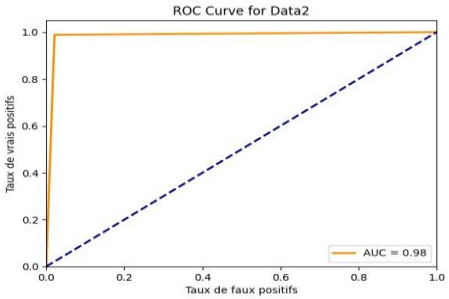

Figure 10. ROC Curve for Smote + Random Forest + Xgboost

Regarding the best combination of techniques, the combination of Neural Network and SMOTE with the Neural Network classifier is particularly effective. This combination offers an optimal balance between precision, recall, and F1 score, making it a promising approach for detecting DoS attacks in IoT systems.

Comparing our results with previous studies reveals a notable improvement in precision and recall. Previous work using similar approaches often encountered difficulties in balancing precision and recall. Moreover, unlike previous work, our approach, which combines SMOTE for class balancing and a neural network for feature selection and classification, seems to offer a better compromise between these metrics. We achieved a precision of 0.98, a recall of 0.9913, and an F1 score of 0.9559, effectively balancing precision and recall. Our research proposes a comprehensive methodology integrating feature selection and class balancing, resulting in more robust and reliable results for detecting DoS attacks.

Our study has some limitations. Although we explored several combinations of techniques, other combinations or data preprocessing methods might offer superior performance. Our

evaluation is based on a specific dataset; additional testing on diverse datasets would be beneficial to validate the generalizability of our results. Moreover, our approach does not address real-time attack detection, which could be interesting to consider in practical applications.

For future research, we suggest exploring other class balancing and feature selection techniques and testing the models on a wider range of datasets. It would also be interesting to explore approaches allowing real-time attack detection.

CONCLUSION

This study explored the effectiveness of combining various feature selection, class balancing, and classification techniques in identifying DoS attacks in IoT environments. We found that a combination of DNN for feature selection and SMOTE for balancing data, coupled with the DNN classifier, delivered superior performance. This achieved an optimal balance of precision, recall, and F1 score, thus offering a promising method for enhancing DoS attack detection in IoT systems.

Despite some limitations, such as the absence of real-time detection capabilities and the exclusive use of a specific dataset, our findings contribute to the ongoing discourse on IoT security, suggesting avenues for further research. Future studies could benefit from exploring a broader array of class balancing and feature selection methods, evaluating the models against diverse attack scenarios, and developing solutions for real-time detection.

ACKNOWLEDGEMENT

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) [funding reference number 06351]).

REFERENCES

[1] K. Ashton, "That 'internet of things' thing," *RFID JOURNAL*, 6 2009.

[2] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on internet of things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[3] C. Lyu, X. Zhang, Z. Liu, and C.-H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for internet of things against dos attacks," *IEEE Access*, vol. 7, pp. 31068–31082, 2019.

[4] Z. Ahmad, A. S. Khan, K. Nisar, I. Haider, R. Hassan, M. R. Haque, S. Tarmizi, and J. J. P. C. Rodrigues, "Anomaly detection using deep neural network for iot architecture," *Applied Sciences*, vol. 11, p. 7050, 7 2021.

[5] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems : A survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, 2019.

[6] K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things : A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[7] S. Hanif, T. Ilyas, and M. Zeeshan, "Intrusion detection in iot using artificial neural networks on unsw-15 dataset." IEEE, 10 2019, pp. 152–156.

[8] A. A. Anitha and D. L. Arockiam, "Annids : Artificial neural network based intrusion detection system for internet of things," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, pp. 2583–2588, 9 2019.

[9] K. Goeschel, "Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive bayes for off-line analysis." IEEE, 3 2016, pp. 1–6.

[10] D. Jing and H.-B. Chen, "Svm based network intrusion detection for the unsw-nb15 dataset." IEEE, 10 2019, pp. 1–4.

[11] Z. H. Abdaljabar, O. N. Ucan, and K. M. A. Alheeti, "An intrusion detection system for iot using knn and decision-tree based classification." IEEE, 12 2021, pp. 1–5.

[12] B. Ingre, A. Yadav, and A. K. Soni, *Decision Tree Based Intrusion Detection System for NSL-KDD Dataset*, 2018, pp. 207–218.

[13] K. Rai, M. S. Devi, and A. Guleria, "Decision tree based algorithm for intrusion detection," *Advanced Networking and Applications*, vol. 07, pp. 2828–2834, 2016.

[14] R. Bapat, A. Mandya, X. Liu, B. Abraham, D. E. Brown, H. Kang, and M. Veeraraghavan, "Identifying malicious botnet traffic using logistic regression." IEEE, 4 2018, pp. 266–271.

[15] S. Sambangi and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression," in *The 14th International Conference on Interdisciplinarity in Engineering 2020*. Basel, Switzerland : MDPI, 2020, p. 51.

[16] A. P. Muniyandi, R. Rajeswari, and R. Rajaram, "Network anomaly detection by cascading k-means clustering and c4.5 decision tree algorithm," *Procedia Engineering*, vol. 30, pp. 174–182, 2012.

[17] K. Peng, V. C. M. Leung, and Q. Huang, "Clustering approach based on mini batch kmeans for intrusion detection system over big data," *IEEE Access*, vol. 6, pp. 11897–11906, 2018.

[18] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network." IEEE, 2 2017, pp. 313–316.

[19] H. F. Aliabadi, "A hybrid method for intrusion detection in the iot," *International journal of Web Research*, pp. 55–60, 12 2022.

[20] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in sdn-based networks." IEEE, 6 2018, pp. 202–206.

[21] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection." IEEE, 2 2016, pp. 1–5.

[22] R. Qaddoura, A. M. Al-Zoubi, I. Almomani, and H. Faris, "A multi-stage classification approach for iot intrusion detection based on clustering with oversampling," *Applied Sciences*, vol. 11, p. 3022, 3 2021.

[23] M. I. Alghamdi, "A hybrid model for intrusion detection in iot applications," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–9, 5 2022.

[24] A. Ferdowsi and W. Saad, "Generative adversarial networks for distributed intrusion detection in the internet of things." IEEE, 12 2019, pp. 1–6.

[25] V. Rattan, R. Mittal, J. Singh, and V. Malik, "Analyzing the application of smote on machine learning classifiers." IEEE, 3 2021, pp. 692–695.

[26] J. Prusa, T. M. Khoshgoftaar, D. J. Dittman, and A. Napolitano, "Using random undersampling to alleviate class imbalance on tweet sentiment data." IEEE, 8 2015, pp. 197–202.

[27] J. Cai, J. Luo, S. Wang, and et al., "Feature selection in machine learning : A new perspective," *Neurocomputing*, vol. 300, pp. 70–79, 2018.

[28] M. Bensalem, J. Dizdarevic, and A. Jukan, “Modeling of deep neural network (dnn) placement and inference in edge computing,” in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2020, pp. 1–6.

[29] M. N. Hasan, M. Nasser, S. Ahmad, and et al., “Feature selection for intrusion detection using random forest,” *Journal of Information Security*, vol. 07, no. 03, pp. 129–140, 2016.

[30] N. Alsharif, “Ensembling pca-based feature selection with random tree classifier for intrusion detection on iot network,” in *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2021, pp. 317–321.

CONCLUSION GÉNÉRALE

3.1. RESUME DES OBJECTIFS

La sécurité des données est devenue un enjeu majeur dans le monde de l'IoT, essentiellement lorsque les données sont très sensibles et critiques. Dans l'IoT, garantir et assurer la sécurité des données est l'un des défis les plus difficiles à relever. Les attaques DoS et DDoS sont particulièrement alarmantes, car elles peuvent perturber ou paralyser les réseaux. Ces attaques visent à surcharger le réseau avec un trafic excessif, empêchant les appareils de répondre efficacement aux demandes légitimes, avec des conséquences dévastatrices pour des secteurs critiques tels que les infrastructures industrielles et les systèmes de santé connectés.

La notion de détection d'intrusion est apparue avec les besoins spécifiques en matière de sécurité des systèmes informatiques. Les méthodes traditionnelles sont souvent inadaptées aux spécificités de l'IoT, comme la diversité des appareils et des protocoles, ainsi que leurs contraintes de traitement et de stockage. L'apprentissage automatique s'est avéré comme une approche prometteuse pour développer des systèmes dynamiques capables de contrer efficacement les attaques DoS et DDoS. Bien que de nombreuses études aient exploré la détection des intrusions dans les systèmes IoT à l'aide de l'apprentissage automatique, il reste nécessaire d'améliorer la précision et l'efficacité des modèles de détection face aux attaques DoS.

L'objectif principal de cette recherche est de proposer un modèle d'apprentissage automatique pour détecter efficacement les attaques DoS dans les systèmes IoT.

Nous résumons par la suite dans les sections suivantes le travail accompli, ses limitations ainsi que nos perspectives de développement futur.

3.2. TRAVAIL ACCOMPLI

Dans ce travail de recherche, nous avons exploré l'efficacité de différentes combinaisons de techniques de classification, de sélection de caractéristiques et d'équilibrage de classes pour détecter les attaques DoS dans les systèmes IoT. Plusieurs modèles de classification ont été évalués, notamment SVM, le DNN, XGBoost et Random Forest , chacun affiné grâce à des techniques d'optimisation d'hyperparamètres spécifiques.

Les résultats obtenus ont mis en évidence la performance de la combinaison du DNN avec la technique SMOTE et le classificateur DNN. Cette approche a démontré une capacité à détecter efficacement les attaques DoS tout en maintenant un faible taux de faux positifs, ce qui en fait une solution prometteuse pour renforcer la sécurité des systèmes IoT.

En outre, l'étude a souligné l'importance de l'équilibrage des classes et de la sélection des caractéristiques dans le processus de détection des attaques. En combinant ces deux techniques, nous avons amélioré les performances du modèle par rapport aux approches traditionnelles. Ces résultats contribuent à combler les lacunes de la littérature existante en fournissant une méthodologie fiable pour la détection des attaques DoS dans les systèmes IoT.

3.3. LIMITATION ET PERSPECTIVES FUTURES

Dans cette section, nous passons en revue les limitations de notre modèle de détection d’intrusion. Ensuite, nous soulignons certaines des avenues intéressantes pour les recherches futures dans la section suivante.

Notre approche proposée permet de détecter les attaques DoS dans les systèmes IoT. Bien que notre étude présente certaines limites, telles que le manque de détection en temps réel et le recours à un ensemble de données spécifique, nous pensons que ce travail ouvre la voie vers des nouvelles perspectives et il reste encore du chemin à faire afin d’améliorer et

explorer de nouvelles pistes. Il serait intéressant d'explorer d'autres techniques d'équilibrage de classes et de sélection de fonctionnalités, ainsi que de tester les modèles sur un plus large éventail de types d'attaques et d'ensembles de données. L'exploration de méthodes de détection des attaques en temps réel pourrait également améliorer considérablement l'utilité pratique des systèmes de détection d'intrusion pour les réseaux IoT.

En conclusion, cette recherche apporte une contribution significative à la détection des attaques DoS dans les systèmes IoT et propose une approche améliorée pour renforcer la sécurité de ces systèmes

RÉFÉRENCES BIBLIOGRAPHIQUES

1. K Ashton. That “Internet of Things” Thing. RFID JOURNAL. 2009 Jun 22, p. 97-114 ;

2. Jean-Michel M. Les objectifs des « réseaux futurs» vus par l’UIT. *Photoniques*, 2017, no 89, p. 36-39 ;

3. Corici A, Emmelmann M, Luo J, Shrestha R, Corici M, Magedanz T. IoT inter-security domain trust transfer and service dispatch solution. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE; 2016. p. 694–9;

4. Sha K, Errabelly R, Wei W, Yang TA, Wang Z. EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security. In: 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC). IEEE; 2017. p. 81–8;

5. Al-Sarawi S, Anbar M, Abdullah R, Al Hawari AB. Internet of Things Market Analysis Forecasts, 2020–2030. In: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE; 2020. p. 449–53 ;

6. Issa M, Hassen Ben R. Gateway IoT de pilotage et de surveillance des capteurs domestiques via le protocole MQTT. Colloque sur les Objets et systèmes Connectés 2022, Ecole Supérieure Polytechnique de Dakar, May 2022, Dakar, Sénégal. ⟨hal-04397658⟩ ; 7. Lyu C, Zhang X, Liu Z, Chi CH. Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks. IEEE Access. 2019;p. 7:31068–82;

8. Hossain M, Fotouhi M, Hasan R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In: 2015 IEEE World Congress on Services. IEEE; 2015. p. 21–8.

9. Ahmad Z, Shahid Khan A, Nisar K, Haider I, Hassan R, Haque MR, et al. Anomaly Detection Using Deep Neural Network for IoT Architecture. Applied Sciences. 2021 Jul 30;p. 11(15):7050.

10. Shadi A, Mohammed A, Rosni A, Ahmad B. Al Hawari. Internet of Things Market Analysis Forecasts, 2020–2030. Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). 2020;p. 449–53;

11. Liu H, Lang B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences. 2019 Oct 17; p. 9(20):4396;

12. Islam N, Farhin F, Sultana I, Shamim Kaiser M, Sazzadur Rahman Md, Mahmud M, et al. Towards Machine Learning Based Intrusion Detection in IoT Networks. Computers, Materials & Continua. 2021; p. 69(2):1801–21;

13. Brunel Rolack K, Mehdi A. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. Mdpi, Artificial Intelligence Empowered Internet of Things. 2024 May, DOI: https://doi.org/10.3390/electronics13183601 ;

14. Brunel Rolack K, Mehdi A, Paul C, Igor TH, Amro N. Machine Learning for DoS Attack Detection in IoT Systems. The 21st International Conference on Mobile Systems and Pervasive Computing (MobiSPC) August 5-7, 2024, Marshall University, Huntington, WV, USA. DOI: https://doi.org/10.1016/j.procs.2024.08.027 ;