COLLEGES BRETAGNE LOIRE | SCIENCES POUR L'INGENIEUR ET LE NUMERIQUE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

THÈSE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPÉRIEURE
MINES-TÉLÉCOM ATLANTIQUE BRETAGNE
PAYS DE LA LOIRE – IMT ATLANTIQUE

ÉCOLE DOCTORALE N° 648
Sciences pour l'Ingénieur et le Numérique
Spécialité : *Mathématiques et Sciences et Technologies de l'Information et de la Communication*

Par
Léo LAVAUR

Apprentissage Fédéré pour la Détection Collaborative d'Intrusions

Thèse présentée et soutenue à Rennes, le XX septembre 2024
Unité de recherche : IRISA (UMR 6074), SOTERN

Rapporteurs avant soutenance :

Prénom NOM   Fonction et établissement d'exercice
Prénom NOM   Fonction et établissement d'exercice
Prénom NOM   Fonction et établissement d'exercice

Composition du Jury :

Attention, en cas d'absence d'un des membres du Jury le jour de la soutenance, la composition du jury doit être revue pour s'assurer quelle est conforme et devra être répercutée sur la couverture de thèse

Président :	Prénom NOM	Fonction et établissement d'exercice *(à préciser après la soutenance)*
Examinateurs :	Prénom NOM	Fonction et établissement d'exercice
	Prénom NOM	Fonction et établissement d'exercice
	Prénom NOM	Fonction et établissement d'exercice
	Fabien AUTREL	Ingénieur de recherche à IMT Atlantique
	Marc-Oliver PAHL	Directeur détude à IMT Atlantique
Dir. de thèse :	Yann BUSNEL	Directeur de la Recherche et de l'Innovation (DRI) à IMT Nord Europe

Invité(s) :

Prénom NOM   Fonction et établissement d'exercice

ABSTRACTS

ACKNOWLEDGEMENTS

Table of Contents

List of Figures

Part I

Introduction

Part II

Federated Learning to build CIDSs

Chapter 3

State of the Art

The Evolution of Federated-Learning–based Intrusion Detection and Mitigation

Contents

3.1 Introduction and Motivation

In the previous chapter, we introduced the concepts of intrusion detection system (IDS) and machine learning (ML), the challenges of deploying collaborative IDSs (CIDSs), and why federated learning (FL) is a promising solution to these challenges. This chapter's prime objective is to provide a comprehensive review of how federated learning (FL) can be leveraged for intrusion detection purposes, and shed light on the gaps in the literature that are discussed in this thesis.

A recent topic without identity Because of the novelty of FL in the field of intrusion detection system (IDS), the literature on the topic is still scarce. Only a handful of reviews [**campos_EvaluatingFederatedLearning_2021**; Ala+21; Agr+21] had been published on the topic when we stopped our data collection for this study in late 2021. While these papers provide a good overview of the existing works, they fail to provide synthesis and extract the core characteristics of the field. Notably, *what makes FL for IDS different from FL for other applications, and what challenges are specific to the field of intrusion detection?*

A systematic approach We aim to address this gap as thoroughly and transparently as possible, and leverage the systematic literature review (SLR) methodology to that end. This methodology [KC07] relies on a structured process to identify, select, and analyze the relevant literature on a given topic. With explicitly defined research questions and inclusion/exclusion criteria, the systematic literature review (SLR) methodology ensures that the review is reproducible and unbiased. Therefore, we intend to provide a comprehensive overview of the existing literature, and reproducible, evidence-based conclusions on the specificities of FL for IDS.

The content of this chapter is based on our survey published in TNSM in May 2022 [Lav+22b] and its accompanying extension at the C&ESAR conference in November 2022 [Lav+22a]. Because the initial paper was submitted in November 2021, the quantitative analysis has been updated during the writing of this manuscript to include the latest publications on the topic. The qualitative analysis has also completed to a lesser extent.

Contributions of this chapter

- The first (at the time of its publication) SLR on the use of FL for IDS, including qualitative and quantitative analyses of the literature.
- A generalization of the selected works as a reference architecture for federated intrusion detection systems (FIDSs), providing a starting point for future works on the topic.
- A taxonomy synthesizing the state of the art of FIDS, providing a framework to analyze and compare existing and upcoming literature.
- The main challenges and opportunities in the field, and a set of research directions to address them.

3.2 Methodology

This section details the methodology applied to review the state of the art of FIDSs. The original article follows the SLR methodology introduced to the engineering field by Kitchenham et al. [KC07]. SLR uses analytical methods to answer research questions about the literature on a specific topic. The update to the original article is less structured and more focused on the evolution of the field, so the methodology is adapted accordingly.

3.2.1 Research Questions

3.2.2 Search and Selection Process

3.2.3 Data Extraction and Analysis

3.3 Quantitative Analysis

3.3.1 Evolution of the Topic

3.3.2 Relevant Venues

3.3.3 Active Groups

3.3.4 Topics of Interest

3.4 Qualitative Analysis

3.4.1 Structuring the Literature

3.4.2 Federated Learning for Intrusion Detection

Data Source and Type

Preprocessing

Algorithm location

Algorithm Type

Defense Mechanism

Federation Strategy

Communication

FL Type

Aggregation Strategy

Model Target

Analyzed Dataset

Costs and Metrics

3.5 Discussion

3.5.1 Limitations of this Study

3.5.2 Open Issues and Future Directions

Table 3.1 – *Related literature reviews, their topics, contributions, and number of citations according to Google Scholar (Apr. 2024).* Works marked ∗ were originally available as preprints, and were only published afterward. Works marked ‡ are added for the sake of completeness, but were not included in the initial selection.

Domain	Year	Authors	Contributions: Qualitative analysis	Quantitative analysis	Taxonomy	Reference architecture	Performance evaluation	Research directions	Systematic Literature Review	Cited	Ref.
Security information sharing	2016	Skopik et al.	●	○	○	○	○	●	○	291	[SSF16]
	2018	Tounsi et al.	●	●	○	○	○	●	○	448	[TR18]
	2019	Wagner et al.	●	●	○	○	○	●	○	240	[Wag+19]
	2019	Pala et al.	●	●	○	●	○	●	○	63	[PZ19]
ML for intrusion detection	2016	Buczak et al.	●	○	○	○	○	◐	○	3105	[BG16]
	2018	Meng et al.	●	○	○	○	○	●	○	562	[Men+18]
	2019	Chaabouni et al.	●	○	◐	○	○	●	○	790	[Cha+19]
	2019	da Costa et al.	●	○	○	○	○	●	○	492	[dCos+19]
Collaborative detection	2010	Zhou et al.	●	○	○	○	○	●	○	517	[ZLK10]
	2015	Vasilomanolakis et al.	●	○	●	○	○	●	○	379	[VKF15]
Federated learning	2020	Aledhari et al.	●	○	○	○	○	○	○	517	[Ale+20]
	2020	Lyu et al.	●	○	○	○	○	●	○	∗ 436	[LYY20]
	2020	Shen et al.	●	○	○	○	○	●	○	69	[She+20]
	2021	Mothukuri et al.	●	○	●	○	○	●	○	376	[Mot+21a]
	2021	Lo et al.	●	●	○	○	○	●	●	158	[Lo+21]
FL for intrusion detection	2021	Agrawal et al.	●	○	○	○	○	●	○	∗ 142	[Agr+21]
	2021	Alazab et al.	●	○	○	○	○	●	○	158	[Ala+21]
	2021	Campos et al.	●	○	○	○	●	●	○	∗ 123	[Cam+22]
	2022	**Lavaur et al.**	●	●	●	●	○	●	●	22	[Lav+22b]
	2022	Fedorchenko et al. ‡	◐	○	○	○	○	○	○	22	[FNS22]
	2022	Ghimire et al. ‡	●	○	○	○	○	●	○	208	[GR22]
	2024	Isma'ila et al. ‡	●	●	○	○	○	●	●	0	[Ism+24]

● covers topic; ◐ partly addresses topic; ○ does not cover topic.

Cam+22]. Therefore, we extended our search of related works to related topics that were susceptible to share similar challenges or conclusions. This extended selection can be divided into three main categories: (a) security information sharing, (b) intrusion detection, and (c) collaborative machine learning (ML). Table 3.1 provides a summary of this selection, grouped by topic and sorted by publication date. In addition to the initial selection, we also included more recent surveys on the topic [FNS22; GR22; Ism+24], whose number highlights the massive interest in the community.

Common issues of collaborative systems, such as the need for trust, privacy, and security, can also apply to FL-based collaboration systems. Therefore, we include four surveys [SSF16; TR18; Wag+19; PZ19] where the authors discuss the challenges and opportunities of sharing security-related information. They highlight the need for standardization, automation, and incentives, to achieve efficient and effective collaboration. The topic of trust is a clearly identified challenge in these works [Wag19; TR18]. The present study rather focuses on FL as a technical mean for collaboration, but such as trust or incentives are also relevant in this context.

Because ML-based IDS can be considered as a key component of FIDS, we review existing surveys on the topic [BG16; Men+18; Cha+19; dCos+19]. These work cover a wide range of solutions, from traditional ML (support vector machine (SVM), decision tree (DT) and random forest (RF), among others) to more recent approaches, such as deep learning, the latter being overrepresented in the literature of FIDSs. They also provide a good overview of the existing datasets and evaluation metrics, which can be useful for the evaluation of FL-based IDS. However, as noted in Section 3.5.2, typical IDS datasets present limitations that can hinder the evaluation of FL-based IDS.

FL is obviously another critical aspect of FIDSs. Consequently, related works include surveys on the collaborative aspects of ML (b) and FL [Ale+20; Lo+21]. They discuss FL approaches to work with distributed architectures. The security of FL is also heavily reviewed by [She+20; LYY20; Mot+21b]. They identify security threats like communication bottleneck, poisoning, and distributed denial of service (DDoS) attacks, that could endanger FL-based systems. While the IDS use case can be seen as an application of FL, we argue that it raises specific concerns in terms of privacy, latency, and adaptability.

Zhou et al. [ZLK10] and Vasilomanolakis et al. [VKF15] survey the evolution of collaborative IDS (CIDS)—at the merge of intrusion detection (b) and collaborative ML (c). Their works are however older and thus, cannot offer a comprehensive view of CIDS, as FL-based approaches did not exist at the time of their writing. Hence, the authors focus on collaboration in the sense of *detection+correlation*, whereas the analysis presented in this chapter (Section 3.4) surveys the use of FL in IDSs.

Finally, recent work have reviewed the use of FL for intrusion detection [Agr+21; Cam+22; Ala+21]. Alazab et al. [Ala+21] address the wider topic of FL for cybersecurity, which only includes intrusion detection as an application. Their paper is explanatory and provides an overview of FL applications in information security. Like this work, Agrawal et al. [Agr+21] focus on FIDSs, but have different methodology. The authors list existing FIDSs and detail their approaches, and identify open issues. On the other hand, Campos et al. [Cam+22] review a subset of FIDSs by focusing on internet of things (IoT) use case, and the impact of non-IID (independent and identically distributed) data on performance. While all identify challenges and research directions, this work also performs quantitative (Section 3.3) and qualitative (Section 3.4) analyses of existing FIDSs, and extracts reference architecture and taxonomy. The existence of these papers emphasizes the importance and relevance of FIDSs for the research community.

The more recent works on the topic [FNS22; GR22; Ism+24] confirm these observations. The work of Fedorchenko et al. is of little interest, as it only lists and details existing works with close to no added value. Ghimire et al. [GR22] provide a more convincing study, closer to the method applied by Alazab et al. [Ala+21], but with a focus on the IoT. Isma'ila et al. [Ism+24] provide a more comprehensive review and also apply the SLR methodology, while also focusing on the IoT.

3.7 Conclusion

Part III

Quantifying the Limitations of FIDSs

Part IV

Providing Solutions

Part V

Conclusion

Bibliography

[Agr+21] Shaashwat Agrawal et al., « Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions », June 16, 2021, arXiv: 2106.09527 [cs], URL: http://arxiv.org/abs/2106.09527 (visited on 12/02/2021).

[Ala+21] Mamoun Alazab et al., « Federated Learning for Cybersecurity: Concepts, Challenges and Future Directions », *in*: *IEEE Transactions on Industrial Informatics* (2021), pp. 1–1, ISSN: 1551-3203, 1941-0050, DOI: 10/gnm4dj, URL: https://ieeexplore.ieee.org/document/9566732/ (visited on 12/02/2021).

[Ale+20] Mohammed Aledhari et al., « Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications », *in*: *IEEE Access* 8 (2020), pp. 140699–140725, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2020.3013541, URL: https://ieeexplore.ieee.org/document/9153560/.

[BG16] Anna L. Buczak and Erhan Guven, « A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection », *in*: *IEEE Communications Surveys Tutorials* 18.*2* (2016), pp. 1153–1176, ISSN: 1553-877X, DOI: 10.1109/COMST.2015.2494502.

[Cam+22] Enrique Mármol Campos et al., « Evaluating Federated Learning for Intrusion Detection in Internet of Things: Review and Challenges », *in*: *Computer Networks* 203 (Feb. 11, 2022), p. 108661, ISSN: 1389-1286, DOI: 10.1016/j.comnet.2021.108661, URL: https://www.sciencedirect.com/science/article/pii/S1389128621005405 (visited on 04/25/2024).

[Cha+19] Nadia Chaabouni et al., « Network Intrusion Detection for IoT Security Based on Learning Techniques », *in*: *IEEE Communications Surveys & Tutorials* 21.*3* (2019), pp. 2671–2701, ISSN: 1553-877X, DOI: 10.1109/COMST.2019.2896380, URL: https://ieeexplore.ieee.org/document/8629941/.

[dCos+19] Kelton A.P. da Costa et al., « Internet of Things: A Survey on Machine Learning-Based Intrusion Detection Approaches », *in*: *Computer Networks* 151 (Mar. 2019), pp. 147–157, ISSN: 13891286, DOI: 10.1016/j.comnet.2019.01.023, URL: https://doi.org/10.1016/j.comnet.2019.01.023.

[FNS22] Elena Fedorchenko, Evgenia Novikova, and Anton Shulepov, « Comparative Review of the Intrusion Detection Systems Based on Federated Learning: Advantages and Open Challenges », *in*: *Algorithms* 15.*7* (7 July 2022), p. 247, ISSN: 1999-4893, DOI: 10.3390/a15070247, URL: https://www.mdpi.com/1999-4893/15/7/247 (visited on 04/24/2024).

[GR22] Bimal Ghimire and Danda B. Rawat, « Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things », *in*: *IEEE Internet of Things Journal* 9.*11* (June 2022), pp. 8229–8249, ISSN: 2327-4662, DOI: 10.1109/JIOT.2022.3150363, URL: https://ieeexplore.ieee.org/abstract/document/9709603 (visited on 04/12/2024).

[Ism+24] Umar Audi Isma'ila et al., « Review on Approaches of Federated Modeling in Anomaly-Based Intrusion Detection for IoT Devices », *in*: *IEEE Access* 12 (2024), pp. 30941–30961, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2024.3369915, URL: https://ieeexplore.ieee.org/document/10445150 (visited on 04/24/2024).

[KC07] B. Kitchenham and S Charters, *Guidelines for Performing Systematic Literature Reviews in Software Engineering*, EBSE-2007-01, 2007.

[Lav+22a] Leo Lavaur, Benjamin Coste, et al., « Federated Learning as Enabler for Collaborative Security between Not Fully-Trusting Distributed Parties », *in*: *Proceedings of the 29th Computer & Electronics Security Application Rendezvous (C&ESAR): Ensuring Trust in a Decentralized World*, 2022, pp. 65–80, URL: http://ceur-ws.org/Vol-3329/paper-04.pdf.

[Lav+22b] Leo Lavaur, Marc-Oliver Pahl, et al., « The Evolution of Federated Learning-based Intrusion Detection and Mitigation: A Survey », *in*: *IEEE Transactions on Network and Service Management*, Special Issue on Network Security Management (June 2022).

[Lo+21] Sin Kit Lo et al., « A Systematic Literature Review on Federated Machine Learning: From A Software Engineering Perspective », *in*: *ACM Computing Surveys* 54.*5* (June 2021), pp. 1–39, ISSN: 0360-0300, 1557-7341, DOI: 10.1145/3450288, arXiv: 2007.11354, URL: http://arxiv.org/abs/2007.11354 (visited on 10/04/2021).

[LYY20] Lingjuan Lyu, Han Yu, and Qiang Yang, « Threats to Federated Learning: A Survey », *in*: *arXiv* (Mar. 4, 2020), URL: http://arxiv.org/abs/2003.02133.

[Men+18] Weizhi Meng et al., « When Intrusion Detection Meets Blockchain Technology: A Review », *in*: *IEEE Access* 6 (2018), pp. 10179–10188, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2018.2799854, URL: http://ieeexplore.ieee.org/document/8274922/.

[Mot+21a] Viraaji Mothukuri, Prachi Khare, et al., « Federated Learning-based Anomaly Detection for IoT Security Attacks », *in*: *IEEE Internet of Things Journal* (2021), pp. 1–1, ISSN: 2327-4662, DOI: 10/gmhhmw.

[Mot+21b] Viraaji Mothukuri, Reza M. Parizi, et al., « A Survey on Security and Privacy of Federated Learning », *in*: *Future Generation Computer Systems* 115 (Feb. 2021), pp. 619–640, ISSN: 0167739X, DOI: 10.1016/j.future.2020.10.007, URL: https://doi.org/10.1016/j.future.2020.10.007.

[PZ19] Ali Pala and Jun Zhuang, « Information Sharing in Cybersecurity: A Review », *in*: *Decision Analysis* 16.*3* (Sept. 2019), pp. 172–196, ISSN: 1545-8490, DOI: 10.1287/deca.2018.0387, URL: http://pubsonline.informs.org/doi/10.1287/deca.2018.0387.

[She+20] Sheng Shen et al., « From Distributed Machine Learning To Federated Learning: In The View Of Data Privacy And Security », *in*: *Concurrency and Computation: Practice and Experience* (Sept. 23, 2020), cpe.6002, ISSN: 1532-0626, 1532-0634, DOI: 10.1002/cpe.6002, arXiv: 2010.09258, URL: http://arxiv.org/abs/2010.09258 (visited on 10/04/2021).

[SSF16] Florian Skopik, Giuseppe Settanni, and Roman Fiedler, « A Problem Shared Is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing », *in*: *Computers & Security* 60 (2016), pp. 154–176, ISSN: 01674048, DOI: 10.1016/j.cose.2016.04.003.

[TR18] Wiem Tounsi and Helmi Rais, « A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks », *in*: *Computers & Security* 72 (Jan. 2018), pp. 212–233, ISSN: 01674048, DOI: 10.1016/j.cose.2017.09.001, URL: https://doi.org/10.1016/j.cose.2017.09.001.

[VKF15] Emmanouil Vasilomanolakis, Shankar Karuppayah, and Mathias Fischer, « Taxonomy and Survey of Collaborative Intrusion Detection », *in*: *ACM Computing Surveys* 47.*4* (May 2015), p. 33, DOI: 10.1145/2716260.

[Wag+19] Thomas D. Wagner et al., « Cyber Threat Intelligence Sharing: Survey and Research Directions », *in*: *Computers & Security* 87 (2019), p. 101589, ISSN: 01674048, DOI: 10.1016/j.cose.2019.101589.

[Wag19] Thomas D Wagner, « Cyber Threat Intelligence for “Things” », *in*: *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, IEEE, June 2019, pp. 1–2, ISBN: 978-1-72810-232-0, DOI: 10.1109/CyberSA.2019.8899384, URL: https://ieeexplore.ieee.org/document/8899384/.

[ZLK10] Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera, « A Survey of Coordinated Attacks and Collaborative Intrusion Detection », *in*: *Computers & Security* 29.*1* (Feb. 2010), pp. 124–140, ISSN: 01674048, DOI: 10.1016/j.cose.2009.06.008, URL: https://linkinghub.elsevier.com/retrieve/pii/S016740480900073X (visited on 07/21/2021).

Appendices

A Résumé en français de la thèse

COLLEGES BRETAGNE LOIRE | SCIENCES POUR L'INGENIEUR ET LE NUMERIQUE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Titre : titre (en français)..............

Mot clés : de 3 à 6 mots clefs

Résumé : Eius populus ab incunabulis primis ad usque pueritiae tempus extremum, quod annis circumcluditur fere trecentis, circummurana pertulit bella, deinde aetatem ingressus adultam post multiplices bellorum aerumnas Alpes transcendit et fretum, in iuvenem erectus et virum ex omni plaga quam orbis ambit inmensus, reportavit laureas et triumphos, iamque vergens in senium et nomine solo aliquotiens vincens ad tranquilliora vitae discessit. Hoc inmaturo interitu ipse quoque sui pertaesus excessit e vita aetatis nono anno atque vicensimo cum quadriennio imperasset. natus apud Tuscos in Massa Veternensi, patre Constantio Constantini fratre imperatoris, matreque Galla. Thalassius vero ea tempestate praefectus praetorio praesens ipse quoque adrogantis ingenii, considerans incitationem eius ad multorum augeri discrimina, non maturitate vel consiliis mitigabat, ut aliquotiens celsae potestates iras principum molliverunt, sed adversando iurgandoque cum parum congrueret, eum ad rabiem potius evibrabat, Augustum actus eius exaggerando creberrime docens, idque, incertum qua mente, ne lateret adfectans. quibus mox Caesar acrius efferatus, velut contumaciae quoddam vexillum altius erigens, sine respectu salutis alienae vel suae ad vertenda opposita instar rapidi fluminis irrevocabili impetu ferebatur. Hae duae provinciae bello quondam piratico catervis mixtae praedonum.

Title: titre (en anglais)..............

Keywords: de 3 à 6 mots clefs

Abstract: Eius populus ab incunabulis primis ad usque pueritiae tempus extremum, quod annis circumcluditur fere trecentis, circummurana pertulit bella, deinde aetatem ingressus adultam post multiplices bellorum aerumnas Alpes transcendit et fretum, in iuvenem erectus et virum ex omni plaga quam orbis ambit inmensus, reportavit laureas et triumphos, iamque vergens in senium et nomine solo aliquotiens vincens ad tranquilliora vitae discessit. Hoc inmaturo interitu ipse quoque sui pertaesus excessit e vita aetatis nono anno atque vicensimo cum quadriennio imperasset. natus apud Tuscos in Massa Veternensi, patre Constantio Constantini fratre imperatoris, matreque Galla. Thalassius vero ea tempestate praefectus praetorio praesens ipse quoque adrogantis ingenii, considerans incitationem eius ad multorum augeri discrimina, non maturitate vel consiliis mitigabat, ut aliquotiens celsae potestates iras principum molliverunt, sed adversando iurgandoque cum parum congrueret, eum ad rabiem potius evibrabat, Augustum actus eius exaggerando creberrime docens, idque, incertum qua mente, ne lateret adfectans. quibus mox Caesar acrius efferatus, velut contumaciae quoddam vexillum altius erigens, sine respectu salutis alienae vel suae ad vertenda opposita instar rapidi fluminis irrevocabili impetu ferebatur. Hae duae provinciae bello quondam piratico catervis mixtae praedonum.