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 Nº 648
Sciences pour l'Ingénieur et le Numérique
Spécialité : *Sciences et technologies de l'information et de la communication*

Par
Léo LAVAUR

Améliorer la détection d'intrusions dans des systèmes distribués grâce à l'apprentissage fédéré

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

Rapporteurs avant soutenance :

Anne-Marie Kermarrec	Professeure à l'Université Polytechnique Fédérales de Lausanne (EPFL)
Éric Totel	Professeur à Télécom SudParis

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 :	*À compléter après la soutenance.*	
Examinateurs :	Sonia Ben Mokhtar	Directrice de Recherche CNRS au laboratoire LIRIS
	Pierre-François Gimenez	Maître de Conférence à CentraleSupelec
	Vincent Nicomette	Professeur à l'INSA de Toulouse
	Fabien Autrel	Ingénieur de Recherche à IMT Atlantique
	Marc-Oliver Pahl	Directeur d'Études 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

Résumé

La collaboration entre les différents acteurs de la cybersécurité est essentielle pour lutter contre des attaques de plus en plus sophistiquées et nombreuses. Pourtant, les organisations sont souvent réticentes à partager leurs données, par peur de compromettre leur confidentialité, et ce même si cela pourrait d'améliorer leurs modèles de détection d'intrusions. L'apprentissage fédéré est un paradigme récent en apprentissage automatique qui permet à des clients distribués d'entraîner un modèle commun sans partager leurs données. Ces propriétés de collaboration et de confidentialité en font un candidat idéal pour des applications sensibles comme la détection d'intrusions. Si un certain nombre d'applications ont montré qu'il est, en effet, possible d'entraîner un modèle unique sur des données distribuées de détection d'intrusions, peu se sont intéressées à l'aspect collaboratif de ce paradigme. En plus de l'aspect collaboratif, d'autres problématiques apparaissent dans ce contexte, telles que l'hétérogénéité des données des différents participants ou la gestion de participants non fiables. Dans ce manuscrit, nous explorons l'utilisation de l'apprentissage fédéré pour construire des systèmes collaboratifs de détection d'intrusions. En particulier, nous explorons l'impact de la qualité des données dans des contextes hétérogènes, certains types d'attaques par empoisonnement, et proposons des outils et des méthodologies pour améliorer l'évaluation de ce type d'algorithmes distribués.

Abstract

Collaboration between different cybersecurity actors is essential to fight against increasingly sophisticated and numerous attacks. However, stakeholders are often reluctant to share their data, fearing confidentiality and privacy issues, although it would improve their intrusion detection models. Federated learning is a recent paradigm in machine learning that allows distributed clients to train a common model without sharing their data. These properties of collaboration and confidentiality make it an ideal candidate for sensitive applications such as intrusion detection. While several applications have shown that it is indeed possible to train a single model on distributed intrusion detection data, few have focused on the collaborative aspect of this paradigm. In addition to the collaborative aspect, other challenges arise in this context, such as the heterogeneity of the data between different participants or the management of untrusted contributions. In this manuscript, we explore the use of federated learning to build collaborative intrusion detection systems. In particular, we explore the impact of data quality in heterogeneous contexts, some types of poisoning attacks, and propose tools and methodologies to improve the evaluation of these types of distributed algorithms.

ACKNOWLEDGEMENTS

Table of Contents

Part I

Federated Learning to build CIDSs

Chapter 4

Application – FIDSs Performance and Limitations

Part II

Quantifying the Limitations of FIDSs

Part III

Providing Solutions

Bibliography

[16] *Directive (EU) 2016/1148 of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*, 2016, URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[22] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, Dec. 14, 2022, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (visited on 05/26/2024).

[AAA16] Iman Almomani, Bassam Al-Kasasbeh, and Mousa AL-Akhras, « WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks », *in*: *Journal of Sensors* 2016 (2016), pp. 1–16, ISSN: 1687-725X, 1687-7268, DOI: 10.1155/2016/4731953, URL: https://www.hindawi.com/journals/js/2016/4731953/ (visited on 10/25/2021).

[ACA20] Noor Ali Al-Athba Al-Marri, Bekir S. Ciftler, and Mohamed M. Abdallah, « Federated Mimic Learning for Privacy Preserving Intrusion Detection », *in*: *2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), May 2020, pp. 1–6, DOI: 10.1109/BlackSeaCom48709.2020.9234959, URL: https://ieeexplore.ieee.org/document/9234959 (visited on 04/12/2024).

[Agr+22] Shaashwat Agrawal *et al.*, « Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions », *in*: *Computer Communications* 195 (Nov. 1, 2022), pp. 346–361, ISSN: 0140-3664, DOI: 10.1016/j.comcom.2022.09.012, URL: https://www.sciencedirect.com/science/article/pii/S0140366422003516 (visited on 06/09/2024).

[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/.

[Ali+18] Janne Ali-Tolppa *et al.*, « SELF-HEALING AND RESILIENCE IN FUTURE 5G COGNITIVE AUTONOMOUS NETWORKS », *in*: *2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K)*, 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K), Santa Fe: IEEE, Nov. 2018, pp. 1–8, ISBN: 978-92-61-26921-0, DOI: 10.23919/ITU-WT.2018.8598115, URL: https://ieeexplore.ieee.org/document/8598115/ (visited on 03/31/2022).

[And+18] Elli Androulaki *et al.*, « Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains », *in*: *Proceedings of the Thirteenth EuroSys Conference*, New York, NY, USA: ACM, Apr. 23, 2018, pp. 1–15, ISBN: 978-1-4503-5584-1, DOI: 10.1145/3190508.3190538, URL: https://dl.acm.org/doi/10.1145/3190508.3190538.

[APB20] Ons Aouedi, Kandaraj Piamrat, and Dhruvjyoti Bagadthey, « A Semi-supervised Stacked Autoencoder Approach for Network Traffic Classification », *in*: *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, 2020 IEEE 28th International Conference on Network Protocols (ICNP), Oct. 2020, pp. 1–6, DOI: 10.1109/ICNP49622.2020.9259390, URL: https://ieeexplore.ieee.org/document/9259390 (visited on 06/19/2024).

[Arp+22] Daniel Arp *et al.*, « Dos and Don'ts of Machine Learning in Computer Security », *in*: *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA: USENIX Association, Aug. 2022, pp. 3971–3988, ISBN: 978-1-939133-31-1, URL: https://www.usenix.org/conference/usenixsecurity22/presentation/arp.

[Baj+17] Vaibhav Bajpai *et al.*, « Challenges with Reproducibility », *in*: *Proceedings of the Reproducibility Workshop*, SIGCOMM '17: ACM SIGCOMM 2017 Conference, Los Angeles CA USA: ACM, Aug. 11, 2017, pp. 1–4, ISBN: 978-1-4503-5060-0, DOI: 10.1145/3097766.3097767, URL: https://dl.acm.org/doi/10.1145/3097766.3097767 (visited on 08/12/2022).

[Ber+18] Jeremy Bernstein *et al.*, « signSGD: Compressed Optimisation for Non-Convex Problems », *in*: *Proceedings of the 35th International Conference on Machine Learning*, ed. by Jennifer Dy and Andreas Krause, vol. 80, Proceedings of Machine Learning Research, PMLR, July 10–15, 2018, pp. 560–569, URL: https://proceedings.mlr.press/v80/bernstein18a.html.

[Beu+20] Daniel J Beutel *et al.*, « Flower: A Friendly Federated Learning Research Framework », 2020, arXiv: 2007.14390.

[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.

[BG17] Suman Sankar Bhunia and Mohan Gurusamy, « Dynamic Attack Detection and Mitigation in IoT Using SDN », *in*: *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC: IEEE, Nov. 2017, pp. 1–6, ISBN: 978-1-5090-6796-1, DOI: 10.1109/ATNAC.2017.8215418, URL: http://ieeexplore.ieee.org/document/8215418/ (visited on 04/09/2022).

[Bha+19] Arjun Nitin Bhagoji *et al.*, « Analyzing Federated Learning through an Adversarial Lens », *in*: *Proceedings of the 36th International Conference on Machine Learning*, International Conference on Machine Learning, PMLR, May 24, 2019, pp. 634–643, URL: https://proceedings.mlr.press/v97/bhagoji19a.html (visited on 02/23/2023).

[Big+14] Elaheh Biglar Beigi *et al.*, « Towards Effective Feature Selection in Machine Learning-Based Botnet Detection Approaches », *in*: *2014 IEEE Conference on Communications and Network Security*, 2014 IEEE Conference on Communications and Network Security (CNS), San Francisco, CA, USA: IEEE, Oct. 2014, pp. 247–255, ISBN: 978-1-4799-5890-0, DOI: 10.1109/CNS.2014.6997492, URL: https://ieeexplore.ieee.org/document/6997492 (visited on 10/25/2021).

[Bon+17] Keith Bonawitz, Vladimir Ivanov, *et al.*, « Practical Secure Aggregation for Privacy-Preserving Machine Learning », *in*: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 30, 2017, pp. 1175–1191, ISBN: 978-1-4503-4946-8, DOI: 10.1145/3133956.3133982, URL: https://dl.acm.org/doi/10.1145/3133956.3133982.

[Bon+19] Keith Bonawitz, Hubert Eichner, *et al.*, « Towards Federated Learning at Scale: System Design », *in*: *arXiv* (Feb. 4, 2019), URL: http://arxiv.org/abs/1902.01046.

[Cai+22] Luxin Cai *et al.*, « Cluster-Based Federated Learning Framework for Intrusion Detection », *in*: *2022 IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 2022 IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nov. 2022, pp. 1–6, DOI: 10.1109/PAAP56126.2022.10010553, URL: https://ieeexplore.ieee.org/abstract/document/10010553 (visited on 04/12/2024).

[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).

[CBK09] Varun Chandola, Arindam Banerjee, and Vipin Kumar, « Anomaly Detection: A Survey », *in*: *ACM Computing Surveys* 41.*3* (July 2009), pp. 1–58, ISSN: 0360-0300, 1557-7341, DOI: 10.1145/1541880.1541882, URL: https://dl.acm.org/doi/10.1145/1541880.1541882 (visited on 03/20/2022).

[Cet+19] Burak Cetin *et al.*, « Federated Wireless Network Intrusion Detection », *in*: *2019 IEEE International Conference on Big Data (Big Data)*, 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA: IEEE, Dec. 2019, pp. 6004–6006, ISBN: 978-1-72810-858-2, DOI: 10.1109/BigData47090.2019.9005507, URL: https://ieeexplore.ieee.org/document/9005507/ (visited on 10/25/2021).

[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/.

[Che+20] Zhuo Chen, Na Lv, *et al.*, « Intrusion Detection for Wireless Edge Networks Based on Federated Learning », *in*: *IEEE Access* 8 (2020), pp. 217463–217472, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2020.3041793, URL: https://ieeexplore.ieee.org/document/9274294/ (visited on 10/25/2021).

[Che+22] Yanyu Cheng *et al.*, « Federated Transfer Learning With Client Selection for Intrusion Detection in Mobile Edge Computing », *in*: *IEEE Communications Letters* 26.*3* (Mar. 2022), pp. 552–556, ISSN: 1558-2558, DOI: 10.1109/LCOMM.2022.3140273, URL: https://ieeexplore.ieee.org/abstract/document/9668958 (visited on 04/12/2024).

[CJ20] Davide Chicco and Giuseppe Jurman, « The Advantages of the Matthews Correlation Coefficient (MCC) over F1 Score and Accuracy in Binary Classification Evaluation », *in*: *BMC Genomics* 21.*1* (Dec. 2020), p. 6, ISSN: 1471-2164, DOI: 10.1186/s12864-019-6413-7, URL: https://bmcgenomics.

biomedcentral.com/articles/10.1186/s12864-019-6413-7 (visited on 03/11/2022).

[CK21] Zachary Charles and Jakub Konecny, « Convergence and Accuracy Trade-Offs in Federated Learning and Meta-Learning », *in*: (2021), p. 11.

[Cla04] Benoît Claise, *Cisco Systems NetFlow Services Export Version 9*, RFC 3954, RFC Editor, Oct. 2004, DOI: 10.17487/RFC3954, URL: https://www.rfc-editor.org/info/rfc3954.

[Cun+24] Helio N. Cunha Neto *et al.*, « FedSBS: Federated-Learning Participant-Selection Method for Intrusion Detection Systems », *in*: *Computer Networks* 244 (May 1, 2024), p. 110351, ISSN: 1389-1286, DOI: 10.1016/j.comnet.2024.110351, URL: https://www.sciencedirect.com/science/article/pii/S138912862400183X (visited on 04/12/2024).

[CZY20] Yang Chen, Junzhe Zhang, and Chai Kiat Yeo, « Network Anomaly Detection Using Federated Deep Autoencoding Gaussian Mixture Model », *in*: *Machine Learning for Networking*, ed. by Selma Boumerdassi, Éric Renault, and Paul Mühlethaler, Cham: Springer International Publishing, 2020, pp. 1–14, ISBN: 978-3-030-45778-5.

[DAF18] Rohan Doshi, Noah Apthorpe, and Nick Feamster, « Machine Learning DDoS Detection for Consumer Internet of Things Devices », *in*: *2018 IEEE Security and Privacy Workshops (SPW)* (Ml Apr. 11, 2018), pp. 29–35, DOI: 10.1109/SPW.2018.00013, URL: https://ieeexplore.ieee.org/document/8424629/.

[dCal+23] Francisco Lopes de Caldas Filho *et al.*, « Botnet Detection and Mitigation Model for IoT Networks Using Federated Learning », *in*: *Sensors* 23.*14* (14 Jan. 2023), p. 6305, ISSN: 1424-8220, DOI: 10.3390/s23146305, URL: https://www.mdpi.com/1424-8220/23/14/6305 (visited on 04/12/2024).

[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.

[Den+21] Yongheng Deng *et al.*, « FAIR: Quality-Aware Federated Learning with Precise User Incentive and Model Aggregation », *in*: *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, Vancouver, BC, Canada: IEEE, May 10, 2021, pp. 1–10, ISBN: 978-1-66540-325-2, DOI: 10.1109/INFOCOM42981.2021.9488743, URL: https://ieeexplore.ieee.org/document/9488743/ (visited on 03/27/2024).

[Don+20] Ye Dong *et al.*, « EaSTFLy: Efficient and Secure Ternary Federated Learning », *in*: *Computers & Security* 94 (July 2020), p. 101824, ISSN: 01674048, DOI: 10.1016/j.cose.2020.101824, URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404820300985 (visited on 05/18/2021).

[Dou02] John R. Douceur, « The Sybil Attack », *in*: *Peer-to-Peer Systems*, ed. by Peter Druschel, Frans Kaashoek, and Antony Rowstron, Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 2002, pp. 251–260, ISBN: 978-3-540-45748-0, DOI: 10.1007/3-540-45748-8_24.

[Dra+16] Gerard Draper-Gil *et al.*, « Characterization of Encrypted and VPN Traffic Using Time-related Features: » *in*: *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 2nd International Conference on Information Systems Security and Privacy, Rome, Italy: SCITEPRESS - Science and and Technology Publications, 2016, pp. 407–414, ISBN: 978-989-758-167-0, DOI: 10.5220/0005740704070414, URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0005740704070414 (visited on 10/15/2021).

[Duy+21] Phan The Duy *et al.*, « Federated Learning-Based Intrusion Detection in SDN-enabled IIoT Networks », *in*: *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), Dec. 2021, pp. 424–429, DOI: 10.1109/NICS54270.2021.9701525, URL: https://ieeexplore.ieee.org/abstract/document/9701525 (visited on 04/12/2024).

[EA10] Muna Elsadig and Azween Abduallah, « Biological Intrusion Prevention and Self-Healing Model for Network Security », *in*: *2010 Second International Conference on Future Networks*, 2010 Second International Conference on Future Networks (ICFN 2010), Sanya, Hainan: IEEE, Jan. 2010, pp. 337–342, ISBN: 978-1-4244-5666-6 978-0-7695-3940-9, DOI: 10.1109/ICFN.2010.103, URL: https://ieeexplore.ieee.org/document/5431824/ (visited on 03/31/2022).

[ENI14] ENISA, *Actionable Information for Security Incident Response*, 2014, pp. 1–79.

[EO11] Huwaida Tagelsir Elshoush and Izzeldin Mohamed Osman, « Alert Correlation in Collaborative Intelligent Intrusion Detection Systems—A Survey », *in*: *Applied Soft Computing*, Soft Computing for Information System Security 11.7 (Oct. 1, 2011), pp. 4349–4365, ISSN: 1568-4946, DOI: 10.1016/j.asoc.2010.12.004, URL: https://www.sciencedirect.com/science/article/pii/S156849461000311X (visited on 06/22/2024).

[ERJ21] Gints Engelen, Vera Rimmer, and Wouter Joosen, « Troubleshooting an Intrusion Detection Dataset: The CICIDS2017 Case Study », *in*: *2021 IEEE Security and Privacy Workshops (SPW)*, 2021 IEEE Security and Privacy Workshops (SPW), May 2021, pp. 7–12, DOI: 10.1109/SPW53761.2021.00009, URL: https://ieeexplore.ieee.org/document/9474286 (visited on 06/14/2024).

[Fan+20a] Yulin Fan *et al.*, « IoTDefender: A Federated Transfer Learning Intrusion Detection Framework for 5G IoT », *in*: *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), Guangzhou, China: IEEE, Dec. 2020, pp. 88–95, ISBN: 978-1-66540-396-2, DOI: 10.1109/BigDataSE50710.2020.00020, URL: https://ieeexplore.ieee.org/document/9343358/ (visited on 10/04/2021).

[Fan+20b] Minghong Fang *et al.*, « Local Model Poisoning Attacks to Byzantine-Robust Federated Learning », *in*: 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1605–1622, ISBN: 978-1-939133-17-5, URL: https://www.usenix.org/conference/usenixsecurity20/presentation/fang (visited on 02/23/2023).

[Far+20] Omair Faraj *et al.*, « Taxonomy and Challenges in Machine Learning-Based Approaches to Detect Attacks in the Internet of Things », *in*: *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES 2020: The 15th International Conference on Availability, Reliability and Security, Virtual Event Ireland: ACM, Aug. 25, 2020, pp. 1–10, ISBN: 978-1-4503-8833-7, DOI: 10.1145/3407023.3407048, URL: https://dl.acm.org/doi/10.1145/3407023.3407048 (visited on 06/23/2021).

[Fer+22] Mohamed Amine Ferrag *et al.*, « Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning », *in*: *IEEE Access* 10 (2022), pp. 40281–40306, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2022.3165809, URL: https://ieeexplore.ieee.org/document/9751703 (visited on 04/12/2024).

[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).

[FPS10] Gianluigi Folino, Clara Pizzuti, and Giandomenico Spezzano, « An Ensemble-Based Evolutionary Framework for Coping with Distributed Intrusion Detection », *in*: *Genetic Programming and Evolvable Machines* 11.*2* (June 1, 2010), pp. 131–146, ISSN: 1573-7632, DOI: 10.1007/s10710-010-9101-6, URL: https://doi.org/10.1007/s10710-010-9101-6 (visited on 06/23/2024).

[Fri+23] Othmane Friha *et al.*, « 2DF-IDS: Decentralized and Differentially Private Federated Learning-Based Intrusion Detection System for Industrial IoT », *in*: *Computers & Security* 127 (Apr. 1, 2023), p. 103097, ISSN: 0167-4048, DOI: 10.1016/j.cose.2023.103097, URL: https://www.sciencedirect.com/science/article/pii/S016740482300007X (visited on 04/12/2024).

[FS16] Gianluigi Folino and Pietro Sabatino, « Ensemble Based Collaborative and Distributed Intrusion Detection Systems: A Survey », *in*: *Journal of Network and Computer Applications* 66 (May 2016), pp. 1–16, ISSN: 10848045, DOI: 10.1016/j.jnca.2016.03.011, URL: https://linkinghub.elsevier.com/retrieve/pii/S1084804516300248 (visited on 06/22/2024).

[FYB20] Clement Fung, Chris J.M. M Yoon, and Ivan Beschastnikh, « The Limitations of Federated Learning in Sybil Settings », *in*: *23rd International Symposium on Research in Attacks, Intrusions and Defenses ({RAID} 2020)*, San Sebastian: {USENIX} Association, Oct. 2020, pp. 301–316, ISBN: 978-1-939133-18-2, URL: https://www.usenix.org/conference/raid2020/presentation/fung.

[Gar+09] P. García-Teodoro *et al.*, « Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges », *in*: *Computers & Security* 28.*1-2* (Feb. 2009), pp. 18–28, ISSN: 01674048, DOI: 10.1016/j.cose.2008.08.003, URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404808000692.

[Gho+07] Debanjan Ghosh *et al.*, « Self-Healing Systems — Survey and Synthesis », *in*: *Decision Support Systems* 42.*4* (Jan. 2007), pp. 2164–2185, ISSN: 01679236, DOI: 10.1016/j.dss.2006.06.011, URL: https://linkinghub.elsevier.com/retrieve/pii/S0167923606000807 (visited on 03/31/2022).

[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).

[Guo+23] Wei Guo *et al.*, « A New Federated Learning Model for Host Intrusion Detection System Under Non-IID Data », *in*: *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Oct. 2023, pp. 494–500, DOI:

10.1109/SMC53992.2023.10393972, URL: https://ieeexplore.ieee.org/document/10393972 (visited on 06/11/2024).

[Hab+17] Arash Habibi Lashkari *et al.*, « Characterization of Tor Traffic Using Time Based Features: » *in*: *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal: SCITEPRESS - Science and Technology Publications, 2017, pp. 253–262, ISBN: 978-989-758-209-7, DOI: 10.5220/0006105602530262, URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006105602530262 (visited on 10/15/2021).

[Hai+01] J W Haines *et al.*, « 1999 DARPA Intrusion Detection Evaluation: Design and Procedures », *in*: (2001), p. 188.

[Han+24] Weixiang Han *et al.*, « Heterogeneous Data-Aware Federated Learning for Intrusion Detection Systems via Meta-Sampling in Artificial Intelligence of Things », *in*: *IEEE Internet of Things Journal* 11.*8* (Apr. 2024), pp. 13340–13354, ISSN: 2327-4662, DOI: 10.1109/JIOT.2023.3337755, URL: https://ieeexplore.ieee.org/abstract/document/10334467 (visited on 04/12/2024).

[Har+17] Stephen Hardy *et al.*, « Private Federated Learning on Vertically Partitioned Data via Entity Resolution and Additively Homomorphic Encryption », Nov. 28, 2017, arXiv: 1711.10677 [cs], URL: http://arxiv.org/abs/1711.10677 (visited on 10/04/2021).

[HC18] David Hand and Peter Christen, « A Note on Using the F-measure for Evaluating Record Linkage Algorithms », *in*: *Statistics and Computing* 28.*3* (May 2018), pp. 539–547, ISSN: 0960-3174, 1573-1375, DOI: 10/gfw6dw, URL: http://link.springer.com/10.1007/s11222-017-9746-6 (visited on 11/10/2021).

[HDH23] Suli He, Chengwen Du, and M. Shamim Hossain, « 6G-enabled Consumer Electronics Device Intrusion Detection with Federated Meta-Learning and Digital Twins in a Meta-Verse Environment », *in*: *IEEE Transactions on Consumer Electronics* (2023), pp. 1–1, ISSN: 1558-4127, DOI: 10.1109/TCE.2023.3321846, URL: https://ieeexplore.ieee.org/abstract/document/10271257 (visited on 04/12/2024).

[Hei+20] Xinhong Hei *et al.*, « A Trusted Feature Aggregator Federated Learning for Distributed Malicious Attack Detection », *in*: *Computers & Security* 99 (Dec. 2020), p. 102033, ISSN: 01674048, DOI: 10.1016/j.cose.2020.102033, URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404820303060 (visited on 10/25/2021).

[Hel+22] Stijn Heldens *et al.*, « Litstudy: A Python Package for Literature Reviews », *in*: *SoftwareX* 20 (Dec. 1, 2022), p. 101207, ISSN: 2352-7110, DOI: 10.1016/j.softx.2022.101207, URL: https://www.sciencedirect.com/science/article/pii/S235271102200125X (visited on 06/06/2024).

[Hid18] Ochiai Hideya, *LAN-Security Monitoring Project*, Whitepaper, 2018, URL: https://lan-security.net/whitepaper.pdf (visited on 10/22/2021).

[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).

[Jin+23] Dong Jin, Shuangwu Chen, *et al.*, « Federated Incremental Learning Based Evolvable Intrusion Detection System for Zero-Day Attacks », *in*: *IEEE Network* 37.*1* (Jan. 2023), pp. 125–132, ISSN: 1558-156X, DOI: 10.1109/MNET.018.2200349, URL: https://ieeexplore.ieee.org/abstract/document/10110017 (visited on 04/12/2024).

[Jin+24] Zhigang Jin, Junyi Zhou, *et al.*, « FL-IIDS: A Novel Federated Learning-Based Incremental Intrusion Detection System », *in*: *Future Generation Computer Systems* 151 (Feb. 1, 2024), pp. 57–70, ISSN: 0167-739X, DOI: 10.1016/j.future.2023.09.019, URL: https://www.sciencedirect.com/science/article/pii/S0167739X23003503 (visited on 04/12/2024).

[Joh+16] Alistair E.W. Johnson *et al.*, « MIMIC-III, a Freely Accessible Critical Care Database », *in*: *Scientific Data* 3.*1* (May 24, 2016), p. 160035, ISSN: 2052-4463, DOI: 10.1038/sdata.2016.35, URL: https://doi.org/10.1038/sdata.2016.35.

[Kai+21] Peter Kairouz *et al.*, « Advances and Open Problems in Federated Learning », Mar. 8, 2021, arXiv: 1912.04977 [cs, stat], URL: http://arxiv.org/abs/1912.04977 (visited on 04/01/2022).

[Kar+20] Sai Praneeth Karimireddy *et al.*, « SCAFFOLD: Stochastic Controlled Averaging for Federated Learning », *in*: *Proceedings of the 37th International Conference on Machine Learning*, International Conference on Machine Learning, PMLR, Nov. 21, 2020, pp. 5132–5143, URL: https://proceedings.mlr.press/v119/karimireddy20a.html (visited on 06/23/2024).

[KC03] J.O. Kephart and D.M. Chess, « The Vision of Autonomic Computing », *in*: *Computer* 36.*1* (Jan. 2003), pp. 41–50, ISSN: 0018-9162, DOI: 10.1109/MC.2003.1160055, URL: http://ieeexplore.ieee.org/document/1160055/.

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

[Kes07] S. Keshav, « How to Read a Paper », *in*: *acm special interest group on data communication* 37.*3* (2007), pp. 83–84.

[KGS21] Muah Kim, Onur Gunlu, and Rafael F Schaefer, « Federated Learning with Local Differential Privacy: Trade-offs between Privacy, Utility, and Communication », *in*: (2021).

[Kho+21] Tran Viet Khoa *et al.*, « Deep Transfer Learning: A Novel Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks », Dec. 2, 2021, arXiv: 2112.00988 [cs], URL: http://arxiv.org/abs/2112.00988 (visited on 01/31/2022).

[Kim+20] Seongwoo Kim, He Cai, *et al.*, « Collaborative Anomaly Detection for Internet of Things Based on Federated Learning », *in*: *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China: IEEE, Aug. 9, 2020, pp. 623–628, ISBN: 978-1-72817-327-6, DOI: 10.1109/ICCC49849.2020.9238913, URL: https://ieeexplore.ieee.org/document/9238913/ (visited on 10/25/2021).

[Kol+16] Constantinos Kolias *et al.*, « Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset », *in*: *IEEE Communications Surveys & Tutorials* 18.*1* (2016), pp. 184–208, ISSN: 1553-877X, DOI: 10.1109/COMST.2015.2402161, URL: http://ieeexplore.ieee.org/document/7041170/.

[Kon+16a] Jakub Konený, H. Brendan McMahan, Daniel Ramage, *et al.*, « Federated Optimization: Distributed Machine Learning for On-Device Intelligence », *in*: (Oct. 8, 2016), pp. 1–38, URL: http://arxiv.org/abs/1610.02527.

[Kon+16b] Jakub Konený, H. Brendan McMahan, Felix X. Yu, *et al.*, « Federated Learning: Strategies for Improving Communication Efficiency », *in*: (Oct. 18, 2016), pp. 1–10, URL: http://arxiv.org/abs/1610.05492.

[Kor+19] Nickolaos Koroniotis *et al.*, « Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset », *in*: *Future Generation Computer Systems* 100 (Nov. 2019), pp. 779–796, ISSN: 0167739X, DOI: 10.1016/j.future.2019.05.041, URL: https://linkinghub.elsevier.com/retrieve/pii/S0167739X18327687 (visited on 10/23/2021).

[Lan+22] Maxime Lanvin *et al.*, « Errors in the CICIDS2017 Dataset and the Significant Differences in Detection Performances It Makes », *in*: *CRiSIS 2022 - International Conference on Risks and Security of Internet and Systems*, Sousse, Tunisia, Dec. 2022, pp. 1–16, URL: https://hal.archives-ouvertes.fr/hal-03775466 (visited on 09/29/2022).

[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).

[LDR19] Eliot Lear, Ralph Droms, and Dan Romascanu, *Manufacturer Usage Description Specification*, RFC 8520, RFC Editor, Mar. 2019, DOI: 10.17487/RFC8520, URL: https://rfc-editor.org/rfc/rfc8520.txt.

[Li+20a] Beibei Li, Yuhao Wu, *et al.*, « DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems », *in*: *IEEE Transactions on Industrial Informatics* 3203.c (2020), pp. 1–1, ISSN: 1551-3203, DOI: 10.1109/TII.2020.3023430, URL: https://ieeexplore.ieee.org/document/9195012/.

[Li+20b] Kun Li, Huachun Zhou, *et al.*, « Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning », *in*: *IEEE Access* 8 (2020), pp. 214852–214865, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2020.3041641, URL: https://ieeexplore.ieee.org/document/9274426/ (visited on 10/25/2021).

[Li+20c] Tian Li, Anit Kumar Sahu, *et al.*, « Federated Optimization in Heterogeneous Networks », Apr. 21, 2020, arXiv: 1812.06127 [cs, stat], URL: http://arxiv.org/abs/1812.06127 (visited on 09/20/2021).

[Liu+20] Lumin Liu, Jun Zhang, S.H. Song, *et al.*, « Client-Edge-Cloud Hierarchical Federated Learning », *in*: *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, ICC 2020 - 2020 IEEE International Conference on Communications (ICC), June 2020, pp. 1–6, DOI: 10.1109/ICC40277.2020.9148862, URL: https://ieeexplore.ieee.org/document/9148862 (visited on 06/23/2024).

[Liu+21] Hong Liu, Shuaipeng Zhang, Pengfei Zhang, *et al.*, « Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing », *in*: *IEEE Transactions on Vehicular Technology* 70.*6* (June 2021), pp. 6073–6084, ISSN: 0018-9545, 1939-9359, DOI: 10.1109/TVT.2021.3076780, URL: https://ieeexplore.ieee.org/document/9420262/ (visited on 10/04/2021).

[LL19] Hongyu Liu and Bo Lang, « Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey », *in*: *Applied Sciences* 9.*20* (Oct. 17, 2019), p. 4396, ISSN: 2076-3417, DOI: 10.3390/app9204396, URL: https://www.mdpi.com/2076-3417/9/20/4396 (visited on 03/11/2022).

[LMK22] Wenjuan Li, Weizhi Meng, and Lam For Kwok, « Surveying Trust-Based Collaborative Intrusion Detection: State-of-the-Art, Challenges and Future Directions », *in*: *IEEE Communications Surveys & Tutorials* 24.*1* (2022), pp. 280–305, ISSN: 1553-877X, DOI: 10.1109/COMST.2021.3139052, URL: https://ieeexplore.ieee.org/document/9663537 (visited on 06/22/2024).

[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.

[Mar+19] Samuel Marchal *et al.*, « AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication », *in*: *IEEE Journal on Selected Areas in Communications* 37.*6* (June 2019), pp. 1402–1412, ISSN: 0733-8716, 1558-0008, DOI: 10.1109/JSAC.2019.2904364, URL: https://ieeexplore.ieee.org/document/8664655/ (visited on 06/04/2021).

[McM+17] Brendan McMahan *et al.*, « Communication-Efficient Learning of Deep Networks from Decentralized Data », *in*: *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, ed. by Aarti Singh and Jerry Zhu, vol. 54, Proceedings of Machine Learning Research, PMLR, Apr. 20–22, 2017, pp. 1273–1282, URL: https://proceedings.mlr.press/v54/mcmahan17a.html.

[Mei+18] Yair Meidan *et al.*, « N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders », *in*: *IEEE Pervasive Computing* 17.*3* (July 2018), pp. 12–22, ISSN: 1536-1268, 1558-2590, DOI: 10.1109/MPRV.2018.

03367731, arXiv: 1805.03409, URL: http://arxiv.org/abs/1805.03409 (visited on 10/23/2021).

[Men+15] Guozhu Meng, Yang Liu, *et al.*, « Collaborative Security: A Survey and Taxonomy », *in*: *ACM Computing Surveys* 48.*1* (July 22, 2015), 1:1–1:42, ISSN: 0360-0300, DOI: 10.1145/2785733, URL: https://doi.org/10.1145/2785733 (visited on 06/22/2024).

[Men+18] Weizhi Meng, Elmar Wolfgang Tischhauser, *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/.

[Mer+23] Mohamed Amine Merzouk *et al.*, « Parameterizing Poisoning Attacks in Federated Learning-Based Intrusion Detection », *in*: *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, New York, NY, USA: Association for Computing Machinery, Aug. 29, 2023, pp. 1–8, ISBN: 9798400707728, DOI: 10.1145/3600160.3605090, URL: https://dl.acm.org/doi/10.1145/3600160.3605090 (visited on 01/29/2024).

[MG14] Thomas Morris and Wei Gao, « Industrial Control System Traffic Data Sets for Intrusion Detection Research », *in*: *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, ed. by Eduardo Bayro-Corrochano and Edwin Hancock, vol. 8827, Cham: Springer International Publishing, 2014, pp. 65–78, ISBN: 978-3-319-12567-1 978-3-319-12568-8, DOI: 10.1007/978-3-662-45355-1_5, URL: http://link.springer.com/10.1007/978-3-662-45355-1_5 (visited on 06/10/2021).

[ML15] Stuart Murdoch and Nick Leaver, « Anonymity vs. Trust in Cyber-Security Collaboration », *in*: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, New York, NY, USA: ACM, Oct. 12, 2015, pp. 27–29, ISBN: 978-1-4503-3822-6, DOI: 10.1145/2808128.2808134, URL: https://dl.acm.org/doi/10.1145/2808128.2808134.

[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.

[Mou+20] Nour Moustafa, Marwa Keshky, *et al.*, « Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications », *in*: *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Dec. 2020, pp. 848–855, DOI: 10.1109/TrustCom50675.2020.00114.

[Mou21] Nour Moustafa, « A New Distributed Architecture for Evaluating AI-based Security Systems at the Edge: Network TON_IoT Datasets », *in*: *Sustainable Cities and Society* 72 (Sept. 1, 2021), p. 102994, ISSN: 2210-6707, DOI: 10.1016/j.scs.2021.102994, URL: https://www.sciencedirect.com/science/article/pii/S2210670721002808 (visited on 06/21/2024).

[MS15] Nour Moustafa and Jill Slay, « UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set) », *in*: *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015 Military Communications and Information Systems Conference (MilCIS), Nov. 2015, pp. 1–6, DOI: 10.1109/MilCIS.2015.7348942, URL: https://ieeexplore.ieee.org/abstract/document/7348942 (visited on 10/09/2023).

[Nat24] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, Gaithersburg, MD: National Institute of Standards and Technology, Feb. 26, 2024, NIST CSWP 29, DOI: 10.6028/NIST.CSWP.29, URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (visited on 05/23/2024).

[NDG22] Evgenia Novikova, Elena Doynikova, and Sergey Golubev, « Federated Learning for Intrusion Detection in the Critical Infrastructures: Vertically Partitioned Data Use Case », *in*: *Algorithms* 15.*4* (4 Mar. 23, 2022), p. 104, ISSN: 1999-4893, DOI: 10.3390/a15040104, URL: https://www.mdpi.com/1999-4893/15/4/104 (visited on 07/05/2022).

[Ngu+19] Thien Duc Nguyen, Samuel Marchal, *et al.*, « DÏoT: A Federated Self-learning Anomaly Detection System for IoT », *in*: *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, vol. 2019-July, IEEE, July 2019, pp. 756–767, ISBN: 978-1-72812-519-0, DOI: 10.1109/ICDCS.2019.00080, URL: https://ieeexplore.ieee.org/document/8884802/.

[Ngu+20] Thien Duc Nguyen, Phillip Rieger, Markus Miettinen, *et al.*, « Poisoning Attacks on Federated Learning-based IoT Intrusion Detection System », *in*: *Proceedings 2020 Workshop on Decentralized IoT Systems and Security*, Workshop on Decentralized IoT Systems and Security, San Diego, CA: Internet Society, 2020, ISBN: 978-1-891562-64-8, DOI: 10.14722/diss.2020.

23003, URL: https://www.ndss-symposium.org/wp-content/uploads/2020/04/diss2020-23003-paper.pdf (visited on 01/29/2024).

[Ngu+21] Thien Duc Nguyen, Phillip Rieger, Hossein Yalame, *et al.*, « FLGUARD: Secure and Private Federated Learning », Jan. 21, 2021, arXiv: 2101.02281 [cs], URL: http://arxiv.org/abs/2101.02281 (visited on 05/18/2021).

[Ngu+22] Thien Duc Nguyen, Phillip Rieger, Huili Chen, *et al.*, « FLAME: Taming Backdoors in Federated Learning », *in*: 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 1415–1432, ISBN: 978-1-939133-31-1, URL: https://www.usenix.org/conference/usenixsecurity22/presentation/nguyen (visited on 03/06/2024).

[OWN21] Yazan Otoum, Yue Wan, and Amiya Nayak, « Federated Transfer Learning-Based IDS for the Internet of Medical Things (IoMT) », *in*: *2021 IEEE Globecom Workshops (GC Wkshps)*, 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain: IEEE, Dec. 2021, pp. 1–6, ISBN: 978-1-66542-390-8, DOI: 10/gpbg4z, URL: https://ieeexplore.ieee.org/document/9682118/ (visited on 01/31/2022).

[PA18] Marc-Oliver Pahl and Francois Xavier Aubet, « All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection », *in*: *14th International Conference on Network and Service Management, CNSM 2018, 1st Workshop on Segment Routing and Service Function Chaining* (2018), pp. 72–80.

[Pai99] Pascal Paillier, « Public-Key Cryptosystems Based on Composite Degree Residuosity Classes », *in*: *Advances in Cryptology — EUROCRYPT '99*, ed. by Jacques Stern, vol. 1592, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 223–238, ISBN: 978-3-540-65889-4, DOI: 10.1007/3-540-48910-X_16, URL: http://link.springer.com/10.1007/3-540-48910-X_16 (visited on 07/05/2021).

[Pan+22] Dinelka Panagoda *et al.*, « Application of Federated Learning in Health Care Sector for Malware Detection and Mitigation Using Software Defined Networking Approach », *in*: *2022 2nd Asian Conference on Innovation in Technology (ASIANCON)*, 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Aug. 2022, pp. 1–6, DOI: 10.1109/ASIANCON55314.2022.9909488, URL: https://ieeexplore.ieee.org/abstract/document/9909488 (visited on 04/12/2024).

[PG22] Trung V. Phan and Tri Gia Nguyen, « FEAR: Federated Cyber-Attack Reaction in Distributed Software-Defined Networks with Deep Q-Network », *in*: *2022 Wireless Telecommunications Symposium (WTS)*, 2022 Wireless

Telecommunications Symposium (WTS), Apr. 2022, pp. 1–7, DOI: 10.1109/WTS53620.2022.9768169.

[Pop+21a] Segun I. Popoola, Ruth Ande, *et al.*, « Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT Edge Devices », *in*: *IEEE Internet of Things Journal* (2021), pp. 1–1, ISSN: 2327-4662, 2372-2541, DOI: 10.1109/JIOT.2021.3100755, URL: https://ieeexplore.ieee.org/document/9499122/ (visited on 10/01/2021).

[Pop+21b] Segun I. Popoola, Guan Gui, *et al.*, « Federated Deep Learning for Collaborative Intrusion Detection in Heterogeneous Networks », *in*: *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Sept. 2021, pp. 1–6, DOI: 10.1109/VTC2021-Fall52928.2021.9625505.

[Pop+22] Segun Popoola, Bamidele Adebisi, *et al.*, *Optimizing Deep Learning Model Hyperparameters for Botnet Attack Detection in IoT Networks*, preprint, Apr. 8, 2022, DOI: 10.36227/techrxiv.19501885.v1, URL: https://www.techrxiv.org/articles/preprint/Optimizing_Deep_Learning_Model_Hyperparameters_for_Botnet_Attack_Detection_in_IoT_Networks/19501885/1 (visited on 04/14/2022).

[Pop+23] Segun I. Popoola, Agbotiname L. Imoize, *et al.*, « Federated Deep Learning for Intrusion Detection in Consumer-Centric Internet of Things », *in*: *IEEE Transactions on Consumer Electronics* (2023), pp. 1–1, ISSN: 1558-4127, DOI: 10.1109/TCE.2023.3347170, URL: https://ieeexplore.ieee.org/abstract/document/10373897 (visited on 04/12/2024).

[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.

[Qin+20a] Qiaofeng Qin, Konstantinos Poularakis, *et al.*, « Line-Speed and Scalable Intrusion Detection at the Network Edge via Federated Learning », *in*: *2020 IFIP Networking Conference (Networking)*, 2020 IFIP Networking Conference (Networking), June 2020, pp. 352–360, URL: https://ieeexplore.ieee.org/document/9142704 (visited on 04/12/2024).

[Qin+20b] Qiaofeng Qin, Konstantinos Poularakis, *et al.*, « Line-Speed and Scalable Intrusion Detection at the Network Edge via Federated Learning », *in*: (June 2020), p. 9.

[QK21] Yang Qin and Masaaki Kondo, « Federated Learning-Based Network Intrusion Detection with a Feature Selection Approach », *in*: *2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia: IEEE, June 12, 2021, pp. 1–6, ISBN: 978-1-66543-897-1, DOI: 10.1109/ICECCE52056.2021.9514222, URL: https://ieeexplore.ieee.org/document/9514222/ (visited on 10/04/2021).

[Quy+22] Nguyen Huu Quyen *et al.*, « Federated Intrusion Detection on Non-IID Data for IIoT Networks Using Generative Adversarial Networks and Reinforcement Learning », *in*: *Information Security Practice and Experience*, ed. by Chunhua Su, Dimitris Gritzalis, and Vincenzo Piuri, Cham: Springer International Publishing, 2022, pp. 364–381, ISBN: 978-3-031-21280-2, DOI: 10.1007/978-3-031-21280-2_20.

[Rah+20] Sawsan Abdul Rahman *et al.*, « Internet of Things Intrusion Detection: Centralized, On-Device, or Federated Learning? », *in*: *IEEE Network* 34.*6* (Nov. 2020), pp. 310–317, ISSN: 0890-8044, 1558-156X, DOI: 10.1109/MNET.011.2000286, URL: https://ieeexplore.ieee.org/document/9183799/ (visited on 06/01/2021).

[Rin+17a] Markus Ring *et al.*, « Creation of Flow-Based Data Sets for Intrusion Detection », *in*: *Journal of Information Warfare* 16.*4* (2017), pp. 41–54, ISSN: 14453312, 14453347, JSTOR: 26504117, URL: https://www.jstor.org/stable/26504117.

[Rin+17b] Markus Ring *et al.*, « Flow-Based Benchmark Data Sets for Intrusion Detection », *in*: *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS)* (2017), pp. 361–369, ISSN: 20488610.

[Rod+23] Nuria Rodríguez-Barroso *et al.*, « Survey on Federated Learning Threats: Concepts, Taxonomy on Attacks and Defences, Experimental Study and Challenges », *in*: *Information Fusion* 90 (Feb. 1, 2023), pp. 148–173, ISSN: 1566-2535, DOI: 10.1016/j.inffus.2022.09.011, URL: https://www.sciencedirect.com/science/article/pii/S1566253522001439 (visited on 09/29/2023).

[RWP19] Shailendra Rathore, Byung Wook Kwon, and Jong Hyuk Park, « BlockSecIoTNet: Blockchain-based Decentralized Security Architecture for IoT Network », *in*: *Journal of Network and Computer Applications* 143 (December 2018 Oct. 2019), pp. 167–177, ISSN: 10848045, DOI: 10.1016/j.jnca.2019.06.019, URL: https://doi.org/10.1016/j.jnca.2019.06.019.

[SA21] Sudipan Saha and Tahir Ahmad, « Federated Transfer Learning: Concept and Applications », Mar. 6, 2021, arXiv: 2010.15561 [cs], URL: http://arxiv.org/abs/2010.15561 (visited on 10/04/2021).

[SB20] Jagdeep Singh and Sunny Behal, « Detection and Mitigation of DDoS Attacks in SDN: A Comprehensive Review, Research Challenges and Future Directions », *in*: *Computer Science Review* 37 (Aug. 2020), p. 100279, ISSN: 15740137, DOI: 10.1016/j.cosrev.2020.100279, URL: https://linkinghub.elsevier.com/retrieve/pii/S1574013720301647 (visited on 04/09/2022).

[SEO21] Yuwei Sun, Hiroshi Esaki, and Hideya Ochiai, « Adaptive Intrusion Detection in the Networking of Large-Scale LANs With Segmented Federated Learning », *in*: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 102–112, ISSN: 2644-125X, DOI: 10.1109/OJCOMS.2020.3044323, URL: https://ieeexplore.ieee.org/document/9296578/ (visited on 10/04/2021).

[Sha+24] Yao Shan *et al.*, « CFL-IDS: An Effective Clustered Federated Learning Framework for Industrial Internet of Things Intrusion Detection », *in*: *IEEE Internet of Things Journal* 11.6 (Mar. 2024), pp. 10007–10019, ISSN: 2327-4662, DOI: 10.1109/JIOT.2023.3324302, URL: https://ieeexplore.ieee.org/abstract/document/10285326 (visited on 04/12/2024).

[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).

[SHG18] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, « Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization », *in*: *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116, ISBN: 978-989-758-282-0, DOI: 10.5220/0006639801080116, URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006639801080116 (visited on 10/14/2021).

[Sig99] SigKDD, *KDD Cup 1999 Dataset*, 1999, URL: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (visited on 04/26/2021).

[SLP22] Mohanad Sarhan, Siamak Layeghy, and Marius Portmann, « Towards a Standard Feature Set for Network Intrusion Detection System Datasets », *in*: *Mobile Networks and Applications* 27.*1* (Feb. 1, 2022), pp. 357–370, ISSN: 1572-8153, DOI: 10.1007/s11036-021-01843-0, URL: https://doi.org/10.1007/s11036-021-01843-0 (visited on 04/23/2024).

[Sna+92] Steven R. Snapp *et al.*, « The DIDS (Distributed Intrusion Detection System) Prototype », *in*: *USENIX Summer 1992 Technical Conference (USENIX Summer 1992 Technical Conference)*, San Antonio, TX: USENIX Association, June 1992, URL: https://www.usenix.org/conference/usenix-summer-1992-technical-conference/dids-distributed-intrusion-detection-system.

[SOE20] Yuwei Sun, Hideya Ochiai, and Hiroshi Esaki, « Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs », *in*: *2020 International Joint Conference on Neural Networks (IJCNN)*, 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, United Kingdom: IEEE, July 2020, pp. 1–8, ISBN: 978-1-72816-926-2, DOI: 10.1109/IJCNN48605.2020.9207094, URL: https://ieeexplore.ieee.org/document/9207094/ (visited on 10/01/2021).

[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.

[ST19] William Schneble and Geethapriya Thamilarasu, « Attack Detection Using Federated Learning in Medical Cyber-Physical Systems », *in*: *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, International Conference on Computer Communications and Networks, Aug. 2019.

[Sun+20] Wen Sun, Shiyu Lei, *et al.*, « Adaptive Federated Learning and Digital Twin for Industrial Internet of Things », Oct. 31, 2020, arXiv: 2010.13058 [cs], URL: http://arxiv.org/abs/2010.13058 (visited on 10/04/2021).

[Tan+23] Zhenheng Tang *et al.*, « GossipFL: A Decentralized Federated Learning Framework With Sparsified and Adaptive Communication », *in*: *IEEE Transactions on Parallel and Distributed Systems* 34.*3* (Mar. 2023), pp. 909–922, ISSN: 1558-2183, DOI: 10.1109/TPDS.2022.3230938, URL: https://ieeexplore.ieee.org/document/9996127 (visited on 06/23/2024).

[Tav+09] Mahbod Tavallaee *et al.*, « A Detailed Analysis of the KDD CUP 99 Data Set », *in*: *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, IEEE, July 2009, pp. 1–6, ISBN: 978-1-4244-3763-4, DOI: 10.1109/CISDA.2009.5356528, URL: http://ieeexplore.ieee.org/document/5356528/.

[Thi+22] Huynh Thai Thi *et al.*, « Federated Learning-Based Cyber Threat Hunting for APT Attack Detection in SDN-Enabled Networks », *in*: *2022 21st International Symposium on Communications and Information Technologies (ISCIT)*, 2022 21st International Symposium on Communications and Information Technologies (ISCIT), Sept. 2022, pp. 1–6, DOI: 10.1109/ISCIT55906.2022.9931222, URL: https://ieeexplore.ieee.org/abstract/document/9931222 (visited on 04/12/2024).

[TKM20] Mineto Tsukada, Masaaki Kondo, and Hiroki Matsutani, « A Neural Network-Based On-device Learning Anomaly Detector for Edge Devices », *in*: *IEEE Transactions on Computers* (2020), pp. 1–1, ISSN: 0018-9340, 1557-9956, 2326-3814, DOI: 10.1109/TC.2020.2973631, URL: https://ieeexplore.ieee.org/document/9000710/ (visited on 10/23/2021).

[Tol+20] Vale Tolpegin *et al.*, « Data Poisoning Attacks Against Federated Learning Systems », *in*: *Computer Security – ESORICS 2020*, ed. by Liqun Chen *et al.*, Lecture Notes in Computer Science, Cham: Springer International Publishing, 2020, pp. 480–501, ISBN: 978-3-030-58951-6, DOI: 10.1007/978-3-030-58951-6_24.

[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.

[Vy+21] Nguyen Chi Vy *et al.*, « Federated Learning-Based Intrusion Detection in the Context of IIoT Networks: Poisoning Attack and Defense », *in*: *Network and System Security*, ed. by Min Yang, Chao Chen, and Yang Liu, vol. 13041, Cham: Springer International Publishing, 2021, pp. 131–147, ISBN: 978-3-030-92707-3 978-3-030-92708-0, DOI: 10.1007/978-3-030-92708-0_8, URL: https://link.springer.com/10.1007/978-3-030-92708-0_8 (visited on 03/05/2024).

[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/.

[Wan+22] Ning Wang, Yang Xiao, *et al.*, « FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations », *in*: *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '22: ACM Asia Conference on Computer and Communications Security, Nagasaki Japan: ACM, May 30, 2022, pp. 946–958, ISBN: 978-1-4503-9140-5, DOI: 10.1145/3488932.3517395, URL: https://dl.acm.org/doi/10.1145/3488932.3517395 (visited on 07/05/2022).

[WK21] Yuwei Wang and Burak Kantarci, « Reputation-Enabled Federated Learning Model Aggregation in Mobile Platforms », *in*: *ICC 2021 - IEEE International Conference on Communications*, ICC 2021 - IEEE International Conference on Communications, June 2021, pp. 1–6, DOI: 10.1109/ICC42927.2021.9500928.

[Yad19] Omry Yadan, *Hydra - A Framework for Elegantly Configuring Complex Applications*, Github, 2019, URL: https://github.com/facebookresearch/hydra.

[Yan+19] Qiang Yang, Yang Liu, *et al.*, « Federated Machine Learning: Concept and Applications », *in*: *ACM Transactions on Intelligent Systems and Technology* 10.*2* (Feb. 28, 2019), pp. 1–19, ISSN: 2157-6904, DOI: 10.1145/3298981, URL: https://dl.acm.org/doi/10.1145/3298981.

[Yan+23] Run Yang, Hui He, *et al.*, « Dependable Federated Learning for IoT Intrusion Detection against Poisoning Attacks », *in*: *Computers & Security* 132 (Sept. 1, 2023), p. 103381, ISSN: 0167-4048, DOI: 10.1016/j.cose.2023.103381, URL: https://www.sciencedirect.com/science/article/pii/S0167404823002912 (visited on 03/04/2024).

[Ye+23] Chuyao Ye *et al.*, « PFedSA: Personalized Federated Multi-Task Learning via Similarity Awareness », *in*: *2023 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, 2023 IEEE International Parallel and Distributed Processing Symposium (IPDPS), May 2023, pp. 480–488,

DOI: 10.1109/IPDPS54959.2023.00055, URL: https://ieeexplore.ieee.org/document/10177489 (visited on 12/05/2023).

[Zha+19] Ying Zhao *et al.*, « Multi-Task Network Anomaly Detection Using Federated Learning », *in*: *Proceedings of the Tenth International Symposium on Information and Communication Technology - SoICT 2019*, The Tenth International Symposium, Hanoi, Ha Long Bay, Viet Nam: ACM Press, 2019, pp. 273–279, ISBN: 978-1-4503-7245-9, DOI: 10.1145/3368926.3369705, URL: http://dl.acm.org/citation.cfm?doid=3368926.3369705 (visited on 06/07/2021).

[Zha+20a] Weishan Zhang, Qinghua Lu, *et al.*, « Blockchain-Based Federated Learning for Device Failure Detection in Industrial IoT », *in*: *IEEE Internet of Things Journal* (Sept. 6, 2020), pp. 1–1, ISSN: 2327-4662, DOI: 10.1109/JIOT.2020.3032544, URL: https://ieeexplore.ieee.org/document/9233457/.

[Zha+20b] Weishan Zhang, Tao Zhou, *et al.*, « Dynamic Fusion Based Federated Learning for COVID-19 Detection », *in*: *arXiv* 14.*8* (Sept. 22, 2020), pp. 1–9, ISSN: 23318422, URL: http://arxiv.org/abs/2009.10401.

[Zha+22] Yuemeng Zhang, Yong Zhang, *et al.*, « Evaluation of Data Poisoning Attacks on Federated Learning-Based Network Intrusion Detection System », *in*: *2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Dec. 2022, pp. 2235–2242, DOI: 10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00330, URL: https://ieeexplore.ieee.org/document/10074658 (visited on 10/31/2023).

[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).

List of Figures

List of Tables

COLLEGES BRETAGNE LOIRE
SCIENCES POUR L'INGENIEUR ET LE NUMERIQUE

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

Titre : Améliorer la détection d'intrusions dans des systèmes distribués grâce à l'apprentissage fédéré

Mot clés : apprentissage automatique, apprentissage fédéré, détection d'intrusions, collaboration, confiance

Résumé : La collaboration entre les différents acteurs de la cybersécurité est essentielle pour lutter contre des attaques de plus en plus sophistiquées et nombreuses. Pourtant, les organisations sont souvent réticentes à partager leurs données, par peur de compromettre leur confidentialité, et ce même si cela pourrait d'améliorer leurs modèles de détection d'intrusions. L'apprentissage fédéré est un paradigme récent en apprentissage automatique qui permet à des clients distribués d'entraîner un modèle commun sans partager leurs données. Ces propriétés de collaboration et de confidentialité en font un candidat idéal pour des applications sensibles comme la détection d'intrusions. Si un certain nombre d'applications ont montré qu'il est, en effet, possible d'entraîner un modèle unique sur des données distribuées de détection d'intrusions, peu se sont intéressées à l'aspect collaboratif de ce paradigme. En plus de l'aspect collaboratif, d'autres problématiques apparaissent dans ce contexte, telles que l'hétérogénéité des données des différents participants ou la gestion de participants non fiables. Dans ce manuscrit, nous explorons l'utilisation de l'apprentissage fédéré pour construire des systèmes collaboratifs de détection d'intrusions. En particulier, nous explorons l'impact de la qualité des données dans des contextes hétérogènes, certains types d'attaques par empoisonnement, et proposons des outils et des méthodologies pour améliorer l'évaluation de ce type d'algorithmes distribués.

Title: Improving Intrusion Detection in Distributed Systems with Federated Learning

Keywords: machine learning, federated learning, intrusion detection, collaboration, trust

Abstract: Collaboration between different cybersecurity actors is essential to fight against increasingly sophisticated and numerous attacks. However, stakeholders are often reluctant to share their data, fearing confidentiality and privacy issues, although it would improve their intrusion detection models. Federated learning is a recent paradigm in machine learning that allows distributed clients to train a common model without sharing their data. These properties of collaboration and confidentiality make it an ideal candidate for sensitive applications such as intrusion detection. While several applications have shown that it is indeed possible to train a single model on distributed intrusion detection data, few have focused on the collaborative aspect of this paradigm. In addition to the collaborative aspect, other challenges arise in this context, such as the heterogeneity of the data between different participants or the management of untrusted contributions. In this manuscript, we explore the use of federated learning to build collaborative intrusion detection systems. In particular, we explore the impact of data quality in heterogeneous contexts, some types

of poisoning attacks, and propose tools and methodologies to improve the evaluation of these types of distributed algorithms.