

Decentralized Collaborative Model Learning for Enhanced Distributed Intrusion Detection



By

Zia Ul Islam Nasir

00000398856

Supervisor

Dr. Hassaan Khaliq Qureshi

Department of Engineering

School of Interdisciplinary Engineering & Sciences (SINES)

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

December 2023

Decentralized Collaborative Model Learning for Enhanced Distributed Intrusion Detection



By

Zia Ul Islam Nasir

00000398856

Supervisor

Dr. Hassaan Khaliq Qureshi

A thesis submitted in conformity with the requirements for
the degree of Master of Science in
Computational Science and Engineering

Department of Engineering

School of Interdisciplinary Engineering & Sciences (SINES)

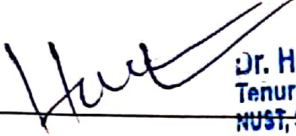
National University of Sciences & Technology (NUST)

Islamabad, Pakistan

December 2023

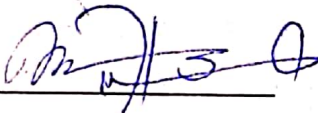
THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS thesis written by Mr. Zia Ul Islam Nasir Registration No. 00000398856 of SINES has been vetted by undersigned, found complete in all aspects as per NUST Statutes/Regulations, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature with stamp:  **Dr. Hassaan Khaliq Qureshi**
Tenured Professor
NUST, School of Electrical Engineering
& Computer Science (SECS)

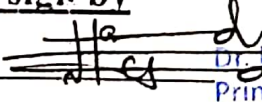
Name of Supervisor: Dr. Hassaan Khaliq Qureshi

Date: 8/11/24

Signature of HoD with stamp:  **Dr. Mian Ilyas Ahmad**
HOD Engineering
Professor
SINES - NUST, Sector H-12
Islamabad

Date: 8/11/2024

Countersign by

Signature (Dean/Principal):  **Dr. Hammad M. Cheema**
Principal & Dean
SINES - NUST, Sector H-12
Islamabad

Date: 09/01/2024

Declaration

I, *Zia Ul Islam Nasir* declare that this thesis titled “Decentralized Collaborative Model Learning for Enhanced Distributed Intrusion Detection” and the work presented in it are my own and has been generated by me as a result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a Master of Science degree at NUST
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at NUST or any other institution, this has been clearly stated
3. Where I have consulted the published work of others, this is always clearly attributed
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work
5. I have acknowledged all main sources of help
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself

Zia Ul Islam Nasir,
00000398856

Copyright Notice

- Copyright in text of this thesis rests with the student author. Copies (by any process) either in full, or of extracts, may be made only in accordance with instructions given by the author and lodged in the Library of SINES, NUST. Details may be obtained by the Librarian. This page must form part of any such copies made. Further copies (by any process) may not be made without the permission (in writing) of the author.
- The ownership of any intellectual property rights which may be described in this thesis is vested in SINES, NUST, subject to any prior agreement to the contrary, and may not be made available for use by third parties without the written permission of SINES, which will prescribe the terms and conditions of any such agreement.
- Further information on the conditions under which disclosures and exploitation may take place is available from the Library of SINES, NUST, Islamabad.

To my beloved parents

℘

*Thousands of children around the world who,
through no fault of their own,
are denied the opportunities for higher education.*

Acknowledgments

At the outset —all glory and praise to Allah Almighty for His countless blessings. In this sacred journey, may His grace continue to illuminate our path, fostering gratitude, resilience, and compassion.

I extend my heartfelt appreciation to my supervisor Professor Dr. Hassaan Khaliq for his consistent support and mentorship during my MS expedition. His invaluable guidance, profound insights, and unwavering encouragement have played a pivotal role in molding the trajectory of my research and aiding me in surmounting the hurdles encountered on this academic odyssey. I consider myself fortunate to have had the opportunity to work with such an exceptional mentor.

I would like to extend my sincerest thanks to my Co-Supervisor Dr. Mian Ilyas Ahmed and evaluation committee members Dr. Mehak Rafiq and Dr. Salma Sherbaz, for their exceptional guidance and mentorship during my research work. I am grateful for their support and guidance throughout my studies.

I would also like to express my deepest gratitude to my parents and siblings for their love, encouragement, and support. Without their sacrifices and understanding, this achievement would not have been possible.

I am grateful to everyone who has contributed to my journey in one way or another.

Abstract

The increasing reliance on networked technologies has triggered a digital transformation in interconnected systems through integrating diverse technologies. This interconnectivity has considerably expanded the attack surface of networks, resulting in a proliferation of cyber-attacks both in number and sophistication. To counteract this trend, the analysis of network traffic through Intrusion Detection Systems (IDS) has emerged as a critical component in the arsenal of network security tools. In response to the escalating rate and complexity of cyber-attacks, researchers have turned to Machine Learning (ML) and Deep Learning (DL) techniques to develop IDS capable of addressing both known and zero-day attacks. While a considerable volume of work has conventionally focused on centralized approaches, this study conducts an empirical investigation of a decentralized learning framework for detecting network intrusions. The proposed scheme adopts a framework that leverages federated learning to surmount the limitations associated with centralized data, integrating federated learning with potent privacy mechanisms, differential privacy to fortify IDS. The analysis of both centralized and decentralized learning scenarios discloses nuanced insights into detection performance. The centralized approach achieves a TPR of 99.51%, followed by 98.05% and 95.31% for the decentralized approach without and with privacy enhancement scheme, respectively. While the centralized approach exhibits slightly better detection performance, its impact on data privacy renders it impractical for real-world implementation. The results underscore the efficiency and efficacy of the designed framework, establishing a model that classifies distinct benign and intrusive traffic patterns from various organizations without requiring inter-organizational data exchange.

Keywords: *Intrusion detection, federated learning, differential privacy, cyber-attacks, data privacy, collaborative learning framework*

Contents

1	Introduction	1
1.1	Background	3
1.2	Motivation	4
1.3	Problem Statement	5
1.4	Objectives	5
1.5	Thesis Organization	6
2	Literature Review	7
2.1	IDS Overview	7
2.1.1	IDS based on Detection Method	8
2.1.2	IDS Based on System Configuration	9
2.2	Related Work	10
2.2.1	Analysis of Recent Development in IDS	10
2.2.2	Threats Taxonomy	14
2.3	Summary	15
3	Methodology	17
3.1	Framework	17
3.2	Data Extraction and Preprocessing	18
3.2.1	Data Extraction	18
3.2.2	Data preprocessing	19

CONTENTS

3.3	Model Initialization	19
3.4	Privacy Preserving	21
3.5	Model Aggregation	23
4	Results and Discussion	25
4.1	Centralized Approach	25
4.2	Decentralized Without PET	26
4.3	Decentralized with PET	28
4.3.1	FedAvg (Federated Averaging)	30
4.3.2	FedAdam (Federated Adam)	31
4.3.3	FedAdagrad (Federated Adaptive Gradient)	32
4.4	Comparison	33
5	Conclusion and Recommendation	36
5.1	Conclusion	36
5.2	Recommendations	37
	References	38

List of Figures

2.1	Anomaly-Based vs Signature Based IDS	8
3.1	The Framework for privacy aware decentralized intrusion detection system	18
3.2	Data preprocessing workflow	19
4.1	Model Performance in Centralized Scenario	27
4.2	Model Performance for Decentralized Approach without PET	29
4.3	Results with FedAvg Aggregation Mechanism.	30
4.4	Results with FedAdam Aggregation Mechanism.	31
4.5	Results with FedAdagrad Aggregation Mechanism.	32
4.6	Comparison of Results in different settings	33
4.7	MAD of decentralized approach with respect to centralized	35
4.8	MSD of decentralized approach with respect to centralized	35

List of Tables

2.1	Overview of Published Works Related to IDS	11
4.1	Model Training Parameters for Centralised Approach	26
4.2	Model Training Parameters for decentralised Approach	28

List of Abbreviations

Abbreviations

ACCS	Australian Centre for Cyber Security
DP	Differential Privacy
FSM	Finite State Machines
IDS	Intrusion Detection System
IP	Internet Protocol
IOC	Indicator of Compromise
NIDS	Network Intrusion Detection System
ML	Machine learning
MAD	Mean Absolute Difference
MSD	Mean Square Difference
PET	Privacy Enhancement Technique

CHAPTER 1

Introduction

As the connected digital world is expanding rapidly, the hazards associated with cybersecurity breaches have increased dramatically [1]. As a result, organizations and governments are actively looking for novel approaches to safeguard personal and organizational data kept on networked devices. However, up until now, computer network security mechanisms have shown themselves to be unreliable in the face of unprecedented attacks [2]. The world's top cyber economy researcher, Cybersecurity Ventures, projects that worldwide cybercrime expenses would increase from USD 3 trillion in 2015 to approximately USD 10.5 trillion annually by 2025 [3]. As a result, there is increasing interest in enhancing the detection controls' present capability to identify sophisticated and unusual threats. Thus, in order to improve intrusion detection systems' performance in detecting attacks, novel and inventive methods are needed.

These interruptions impair the network's capacity to provide its core functions and result in service outages, data loss, damage to the infrastructure, and network failure, all of which have a major negative impact on the economy and society [4, 5]. Network resilience minimizes the effects of attacks by allowing the network to endure disturbances and bounce back swiftly and efficiently [6]. Resilient networks are necessary to minimize service interruption downtime, stop additional harm, and stop cascading failures [7]. Furthermore, a resilient network improves security and increases the difficulty of network disruption or penetration by cybercriminals. Network Intrusion Detection Systems (NIDS) are vital security instruments designed to search for and identify network attackers as they infiltrate a computer network at the perimeter layer [8]. In order to maintain the confidentiality, integrity, and availability—the three pillars of information

system security—NIDS are deployed [9, 10]. For the purpose of identifying patterns and indicators of a possible danger or attack, they monitor and analyze network traffic. The objectives of a network intrusion detection system (NIDS) are to identify security risks, safeguard digital assets, and offer robust cyber-security defense against malicious actors in operational infrastructures [9].

Conventional Network Intrusion Detection Systems (NIDSs) that rely on signatures search and examine incoming network data for any indicator of compromise (IOC), sometimes referred to as attack signatures [11, 12]. The purpose of the detection functionality is to compare the signatures of incoming traffic with a pre-compiled list of known harmful signatures. When the entire collection of IOCs has been previously recognized and recorded within the NIDS, this method offers a high detection accuracy of known and precedented attacks. However, it has been demonstrated to be unreliable against newly discovered attacks (zero-day attacks) or novel variations of known assaults [13], in cases where the IOCs associated with the activity’s occurrence are unknown [14]. Furthermore, the use of classical IOC is insufficient for detecting modern advanced and persistent threats, which call for a sophisticated depth of behavioral change monitoring [15]. In general, attackers quickly and continuously adapt their attack strategies to bypass security protections in place by changing well-known network attack paths. As a result, dynamic attack detection is unavoidable, and NIDSs must be flexible enough to adjust to new methods of attack detection.

Therefore, in order to match attack behaviors and patterns, researchers investigated into anomaly-based NIDSs [14]. Anomaly-based network intrusion detection systems (NIDSs) employ sophisticated statistical techniques to circumvent the drawbacks of signature-based NIDSs, allowing researchers to recognize trends in network traffic behavior. Anomaly detection is accomplished using a variety of approaches, including data, machine, and statistical-based strategies [16]. When it comes to zero-day attacks, they can typically reach better levels of accuracy and Detection Rate (DR) since they concentrate more on matching attack patterns and behaviors [13]. The design and reliable performance assessment of a decentralised and privacy aware intrusion detection systems are the main topics of this thesis. In the last few years, machine learning (ML) techniques have been applied to improve the effectiveness and performance of a wide range of technological applications [17], showing remarkable success in enabling decision-making systems in a variety of areas. As a subset of artificial intelligence (AI) [18, 19],

machine learning (ML) uses a collection of statistical algorithms that are capable of learning from data without explicit programming.

Machine learning (ML) models are acknowledged for their exceptional capacity to extract and learn intricate patterns from data that are not practical for domain experts to observe [20]. During the training phase, machine learning models derive meaningful patterns from past data. Future occurrences and scenarios are predicted, classified, and regressed using the learnt patterns. ML has been a game-changing innovation [21] in a number of sectors where efficiency and operational automation are necessary. The enhanced capabilities of machine learning algorithms and the availability of data have contributed to its current surge in attention [22]. As a result, ML models have been extensively used in a variety of fields, outperforming conventional computing techniques in terms of offering a higher degree of analysis to automate complicated decision-making activities. In order to increase cyber attack detection through the use of an intelligent defense layer and get around the drawbacks of signature-based NIDS, the cyber security domain has also welcomed ML in the development of NIDS [23].

Building on the conversation about how machine learning could transform NIDS, this work takes an innovative approach by adopting federated learning as a decentralized method. Our method deviates from the established framework, where machine learning (ML) was a monumental breakthrough for intrusion detection. This paradigm fosters a collaborative and privacy-centric design process by having individual clients actively contribute on their own data.

1.1 Background

Machine Learning (ML) technologies have achieved widespread adoption across diverse domains and applications, each presenting its own unique set of challenges and considerations. When crafting a learning model, adherence to general guidelines and best practices is crucial. The selection of a specific ML process or technique is contingent upon various factors, including the availability of resources such as training data samples, data sensitivity, heterogeneity of data, computing power, storage requirements, among others. Consequently, the application of ML technologies may vary in ease across different domains, dictated by the intricacies of available resources.

In the realm of ML-based Network Intrusion Detection Systems (NIDS), the paramount concerns revolve around the privacy and security of data samples utilized during training and testing phases. The potential compromise of user information through sharing with third parties poses a significant threat to data privacy. Consequently, the design of ML-based NIDS encounters challenges related to data scarcity, often stemming from limitations in the quantity of collected data samples or insufficient representation of diverse data classes. Moreover, the inherent heterogeneity within network data samples exacerbates the issue of generalization.

In practice, a model trained to achieve high accuracy in one network structure may exhibit diminished effectiveness when applied to detect intrusions in a different network environment. This discrepancy arises from the distinctive Standard Operating Environments (SOEs) present in each organizational network, coupled with variations in the types of threats experienced. These disparities manifest in the statistical distribution of utilized NIDS datasets, highlighting the critical impact of network-specific factors.

In the landscape of ML-based NIDS, where the stakes are elevated due to the critical nature of network security, the ramifications of data scarcity and heterogeneity are pronounced. The limited availability of real-world datasets poses a formidable challenge, hindering the development of robust intrusion detection models. Furthermore, the dynamic nature of network threats necessitates continuous adaptation, accentuating the need for models capable of evolving with the ever-changing threat landscape[24]. This dynamicity introduces an additional layer of complexity, where the efficacy of intrusion detection models is contingent upon their agility in learning and adapting to emerging threats and evolving network structures. Therefore, the exploration of ML scenarios within this context becomes not only a technological imperative but also a strategic endeavor in fortifying network defenses against an evolving array of cyber threats.

1.2 Motivation

The escalation of security breaches in recent years has emerged as a formidable menace, imposing substantial risks on organizations globally. As reported by Cybersecurity Ventures, the frequency and gravity of cyber attacks have surged to alarming proportions, prognosticating a staggering global cost of data breaches, estimated to reach USD 10.5

trillion annually by 2025 [3]. These incursions not only inflict financial ramifications but also engender operational disruptions and compromise the confidentiality of sensitive information.

Traditionally, intrusion detection approaches have tended to adopt centralized structures, exposing vulnerabilities and the risk of data breaches. In response to these concerns, this thesis employs a decentralized approach, augmented by differential privacy, to enhance privacy measures. This methodology not only addresses the limitations of centralized systems but also offer a more robust and privacy-preserving solution for real-world intrusion detection challenges.

1.3 Problem Statement

The constantly evolving network landscape highlights the crucial role of Network Intrusion Detection Systems (NIDS) as essential tools for network security. However, most existing methods are centralized and suffer from inefficiencies in real-time detection of network intrusions. To address these issues, this study proposes an innovative NIDS framework that integrates differential privacy to enhance the model's privacy and ensuring individual privacy.

1.4 Objectives

The fundamental aim of this study is to design a decentralized NIDS that is feasible for practical scenarios. The objectives of this work are:

- To develop a robust and scalable framework that enables distributed intrusion detection systems to collaboratively train and aggregate machine learning models
- To formulate and implement a proficient detection algorithm for distinguishing between normal and abnormal network flows
- Investigate novel techniques to enhance the detection accuracy of distributed intrusion detection systems by leveraging the collective intelligence of multiple clients
- To evaluate the proposed algorithm and measure metrics such as detection accuracy, false positive rates.

1.5 Thesis Organization

The subsequent chapters of the thesis are structured as follows: Chapter 2 presents a thorough literature review, delving into the issues investigated in this study. The preceding research has focused on network intrusion detection through the application of statistical methods, pattern matching, expert systems, and machine learning algorithms. Chapter 3 discusses the proposed methodology and implementation details. Chapter 3 delves into the proposed methodology and provides a detailed discussion of the implementation particulars. In Chapter 4, the attained results following the implementation of the proposed methodology are thoroughly discussed, while Chapter 5 encapsulates the drawn conclusions derived from these outcomes.

Literature Review

The field of cybersecurity research has experienced a shift in focus in recent years from preventing the growing number of cyberattacks to grappling with the intricate nature of intrusion detection. This chapter delves into the multifaceted aspects of Intrusion Detection Systems (IDS) and offers an extensive academic overview of past research conducted in the domain of network security.

2.1 IDS Overview

IDS systems are designed to keep an eye on and analyze other systems' and network activity. Finding abnormalities, invasions, or privacy violations is the aim of intrusion detection systems (IDS). According to Ferrag et al. [25], they come in second to access control, authentication, and encryption methods when it comes to defense. Network Intrusion Detection System (NIDS) or Host Intrusion Detection System (HIDS) are two types of IDS. NIDS keep an eye on how various nodes in a network or its subnetworks communicate with one another. They examine both internal and external communication as well as traffic flow. The packets used in a network's communication between two nodes constitute a traffic flow [26]. When source and destination Internet Protocol (IP) addresses are utilized, a network flow may be two-tuple in nature. A flow is regarded as 4-tuple when the source and destination ports are also utilized; 5-tuple flows also include the protocol used. Both unidirectional and bidirectional traffic flows are possible. In contrast to NIDS, HIDS monitors system internals or nodes, with a particular emphasis on log files, operating system (OS) files, etc. Moreover, they enable the analysis of en-

encrypted communications by monitoring the network connectivity of the node or nodes they are installed on [27]. Instead than depending on payload data or headers, HIDS rely on the content of the packet.

2.1.1 IDS based on Detection Method

There are two important types of IDS based on detection approach: anomaly-based and signature-based. IDS that uses signatures, commonly referred to as Misuse Detection, is based on predetermined signatures that stand in for known intrusions and attacks. As a result, by comparison with known signatures, signature-based intrusion detection systems can identify attacks. However, because their capacity to detect attacks is restricted by the signatures present in the database they utilize, attacks lacking signature patterns—including undiscovered or zero-day attacks—go undetected [12, 28].

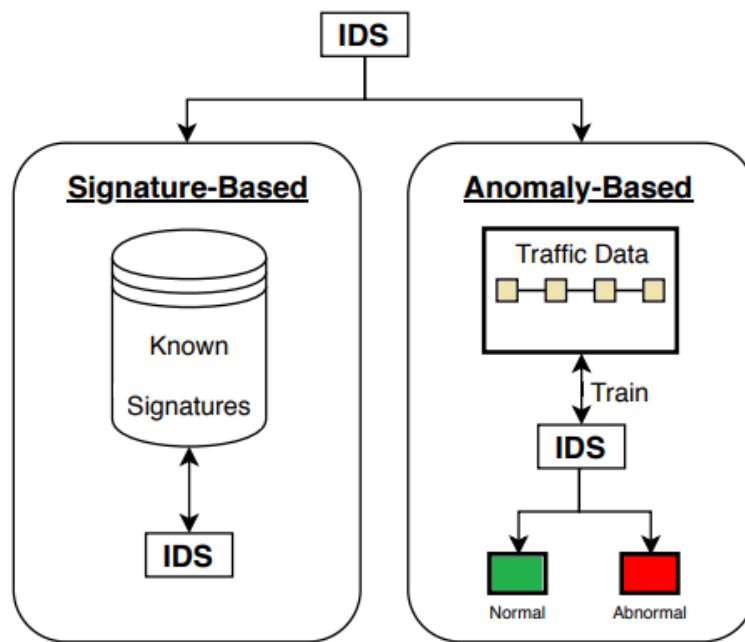


Figure 2.1: Anomaly-Based vs Signature Based IDS

Anomaly-based intrusion detection systems, or "behavior-based detection," on the other hand, rely on pattern recognition[29]. Before the system is deployed, this strategy necessitates training. Because AI methods have substantial training capabilities, Machine Learning (ML) and Deep Learning (DL) in particular are well-suited for anomaly-based intrusion detection systems. Being able to distinguish between regular and abnormal traffic and identify both known and unknown threats is an advantage of anomaly-based

intrusion detection systems[16, 30]. False Positive Rate (FPR) is frequently high, yet anomaly-based intrusion detection systems (IDS) have a higher accuracy rate against unknown threats than signature-based IDS. The strengths of both signature- and anomaly-based techniques are used in specification-based intrusion detection systems (IDS) to create a hybrid model that can try to detect known and unknown threats using various AI techniques. IDS based on anomaly and signature has been compared in Figure 2.1. IDS systems that rely on signatures or anomalies might operate in a stateless or stateful manner. While stateful IDS rely on network flows, stateless IDS rely on packets. Modern IDS are stateful because they take advantage of the context flows. It is important to remember that IDS are reliable for detecting anomalies, not like Intrusion Prevention System (IPS) that can also take preventative and remedial measures as well.

Researchers began utilizing statistical techniques based on predetermined rates in the late 1980s, with typical traffic serving as a baseline for detection. Knowledge-based techniques, such as expert systems and finite state machines (FSM), were employed after statistical techniques. Ultimately, the research and development of IDS was dominated by ML approaches. Current polls highlight the importance of applying ML and DL methods in the development of IDS.

2.1.2 IDS Based on System Configuration

Intrusion detection systems exhibit distinct classifications based on their system structure. A centralized intrusion detection system relies on a singular, centralized authority for monitoring and analysis. In contrast, a distributed intrusion detection system operates across multiple interconnected entities, distributing the monitoring and analysis tasks for enhanced coverage and efficiency.

1. Centralized IDS: A centralized intrusion detection system functions by assessing the overarching state of the network through the consolidation of data from diverse sources. These sources encompass host-based or network-based data collection methods, or a hybrid of both. Subsequently, the accumulated data undergoes central processing and analysis, irrespective of the data sources or sensor locations. This methodology affords a centralized perspective on network security, facilitating thorough analysis and response capabilities from a singular control point.

2. Decentralized IDS: In contrast, a decentralized intrusion detection system entails

the gathering and examination of data across multiple hosts, where decisions are autonomously made at each host. Within a distributed framework, the intrusion detection functionality is dispersed across various points within the network. This methodology provides the benefit of triggering immediate response mechanisms based on local decisions, thereby augmenting the speed of detection and response. However, distributed IDS might exhibit reduced accuracy owing to the absence of global knowledge and coordination, in contrast to centralized systems. Despite these considerations, the decentralized nature of distributed intrusion detection systems introduces a heightened level of adaptability and resilience in complex network environments.

2.2 Related Work

In this section, research articles pertaining to Intrusion Detection Systems (IDS) are comprehensively examined and analyzed, focusing on the diverse datasets employed and the Machine Learning (ML) algorithms utilized for IDS training. Subsequent to the analysis, a synopsis of recently detected cyber attacks by IDS is provided.

2.2.1 Analysis of Recent Development in IDS

This section delves into a comprehensive analysis of recent articles focused on Intrusion Detection Systems (IDS), meticulously examining their strengths, weaknesses, and overarching research trends. A thorough exploration of primary research methodologies and carefully curated datasets is presented, culminating in a nuanced evaluation of the advantages and disadvantages inherent in current IDS implementations. Table 2.1 presents a comprehensive summary of IDS research articles, where each row encapsulates a distinct article. The table provides a detailed overview of the employed datasets, algorithms, and the spectrum of cyber attacks effectively detected by the respective IDS under investigation.

The temporal scope of the table, spanning over a decade, contributes to its significance, capturing the evolving landscape of IDS research. This tabulated presentation serves as a valuable resource for synthesizing key information on the methodologies and outcomes of the analyzed research articles.

Table 2.1: Overview of Published Works Related to IDS

Ref	Used Algorithm	Dataset	Detected Attack	Year
[31]	Tree Classifiers Bayesian Clustering	KDD-99	Probing, DoS, R2L, U2R	2008
[32]	Genetic-based	KDD-99	Probing, DoS, R2L, U2R	2009
[33]	RBF, Elman NN	1999 DARPA	Probing, DoS, R2L, U2R	2009
[34]	AdaBoost	KDD-99	Probing, DoS, R2L, U2R	2009
[35]	FC-ANN based on: ANN Fuzzy Clustering	KDD-99	Probing, DoS, R2L, U2R	2010
[36]	NN FCM Clustering	KDD-99	DoS, R2L, U2R	2010
[37]	OCSVM	Generated dataset	Scan (Nachi, Netbios, SSH), TCP flood, DDoS (TCP, UDP flood), Stealthy DDoS UDP flood, Traffic deletion, Popup spam	2011
[38]	Weighted k-NN Genetic Algorithm	KDD-99	DoS/DDOS	2011
[39]	SOM K-Means clustering	KDD-99	Probing, DoS, R2L, U2R	2011
[40]	SVM	1998 DARPA	Attack, Non-Attack	2012
[41]	Non-Parametric CUSUM	Simulated dataset	Jamming	2013
[42]	NB Classifier K-Means Clustering	ISCX 2012	Normal, Attack	2013
[43]	AIS (NSA, CSA, INA)	NSL-KDD	Normal, Abnormal	2014
[44]	K-Means, k-NN	NSL-KDD	Probing, DoS, R2L, U2R	2015
[45]	ANN	Simulated dataset	DoS/DDoS	2016
[46]	ANN	Generated dataset using httpperf	SQL Injection, XSS	2016
[47]	BON GPU-based ANN	Generated dataset	Normal, Attack	2017
[48]	ANN , SVM	UNB-CIC	nonTor Traffic	2017
[49]	MLP, NB, SVM Logistic Regression RF Features Selection	Simulated dataset	Individual and Combination Routing Attacks: Hello Flood, Sinkhole, Wormhole	2018

Continued ...

Ref	Used Algorithm	Dataset	Detected Attack	Year
[50]	ANN Deep Auto-Encoder	NSL-KDD UNSW-NB15	- Probing, DoS, R2L, U2R Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worm	2018
[51]	DT SVM (least square) Feature Selection: FGLCC, CFA	KDD-99	Probing, DoS, R2l, U2R	2019
[52]	IG, SVM, MLP, PCA, IBK,	ISCX 2012 NSL-KDD Kyoto2006+	Normal, Attack Probing, DoS, R2l, U2R	2019
[53]	DT - NB - MLP - RF - J48 - LSTM - k-NN	CICIDS2017	SSH and FTP Brute-force ,Web Attacks (Brute-force, XSS and SQL Injection)	2020
[54]	Deep NN	NSL-KDD	Probing, DoS, R2l, U2R	2020
[55]	Isolation Forest Local Outlier Factor	Generated dataset	Port Scanning, HTTP and SSH Brute-Force, SYN Flood	2020
[56]	LR, XGB, DT, HCRNN (proposed)	CSE-CIC IDS2018	Brute-force DOS attacks,DDOS attacks, Brute-force SSH, nfiltration, Heartbleed, Web attacks, and Botnet.	2021
[57]	SVM, LDA, RF, NB, LR, HNIDS (proposed)	NSL-KDD UNSW-NB15	Probing, DoS, R2L, U2R Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worm	2022
[58]	DFEL: DT, KNN,SVM	NSL-KDD	Probing, DoS, R2l, U2R	2022

Danish et al. [59] innovatively proposed a LoRaWAN-based Intrusion Detection System (LIDS) tailored for countering jamming attacks. Their methodology involved the creation of a real experimental testbed, training LIDS on authentic join request data using two statistical algorithms: Kullback Leibler Divergence (KLD) and Hamming distance (HD). Through meticulous performance assessments employing Receiver Operating Characteristic (ROC) analysis, the system demonstrated high detection rates. Specifically, KLD achieved up to 98%, while HD reached up to 88%, both maintaining a low 5% false positive rate. These endeavors contribute significantly to the advancement of intrusion detection capabilities in diverse cyber threat scenarios. Gogoi et al. [60] introduced a sophisticated Multi-Level Hybrid Intrusion Detection System (MLH-IDS) that seamlessly integrates supervised, unsupervised, and outlier-based techniques. This

holistic approach aims to enhance the efficiency of intrusion detection, addressing both known and novel zero-day attacks. The performance evaluation of MLH-IDS revealed commendable results, with a detection rate spanning from 81.43% for U2R attacks to an impressive 99.99% for DoS attacks.

McDermott et al. [61] introduced an innovative Intrusion Detection System (IDS) designed specifically for detecting intrusions in Wireless Sensor Networks. The system employs a combination of a backpropagation neural network and a support vector machine (SVM) to enhance detection accuracy. The authors conducted a comprehensive evaluation of the IDS using the NSL-KDD dataset, assessing its performance across six distinct cyber attacks. This research contributes to the evolving landscape of intrusion detection methodologies, showcasing the efficacy of neural network and SVM integration in securing Wireless Sensor Networks against diverse cyber threats.

The impact of using auto encoder and Principal Component Analysis (PCA) on the UNSW-NB15 and NSLKDD datasets were visually examined by the authors in [62]. In a binary and multi-class classification scenario, they also experimented with various dimensions utilizing the classifiers K-Nearest Neighbour (KNN), DFF, and DT. According to the study, for KNN and DFF, AE outperformed PCA, but for DT, both approaches were comparable. It was determined that 20 dimensions was the ideal number for the UNSW-NB15 dataset, but not for the NSL-KDD one. As a method for feature extraction, the authors of [63] suggested an AE neural architecture made up of dense layers and LSTM. To detect attacks, the retrieved output is subsequently fed into an RF classifier. The UNSW-NB15, ToN-IoT, and NSL-KDD datasets were the three used to assess the suggested methodology's performance. The outcomes show that, in the absence of feature extraction techniques, the selected classifier achieves better detection performance. However, employing lesser dimensions has resulted in a considerable reduction in training time.

Khan et al. [64] investigated the five algorithms Decision Trees (DT), Random Forest (RF), Gradient Boosting (GB), AdaBoost, and Naive Bayes (NB) with an additional tree classifier for feature extraction. According to the findings, RF 98.60%, AdaBoost 97.92%, and DT 97.85% had the highest scores. A Convolutional Neural Network (CNN) model was constructed and assessed on the UNSW-NB15 dataset by the authors in [65]. The CNN has a comprehensive set of its hyper-parameters, and it employs max-pooling.

Different numbers of hidden layers as well as the addition of a Long Short Term Memory (LSTM) layer were tested in these experiments. Obtaining accuracy of 85.86% and 91.2%, the three-layer network demonstrated superior performance on both balanced and unbalanced datasets.

2.2.2 Threats Taxonomy

In the realm of intrusion attack classifications, Kendall [66] proposed an influential framework that delineated intrusions into four distinct categories: DoS, R2L, U2R, and Probing. This categorization aligns seamlessly with the timeline of the KDD dataset family, as expounded by Siddique et al.[67]. This historical perspective underscores Kendall’s pivotal role in shaping our comprehension of intrusion types and their resonance with subsequent dataset advancements.

Subsequent to this, various other classifications have emerged in the literature, each honing in on specific facets of attacks or targeting explicit domains. An illustrative instance is the work of Welch and Lathrop [68], which categorizes threats in wireless networks based on attack techniques, delineating seven distinct categories: Traffic Analysis, Passive Eavesdropping, Active Eavesdropping, Unauthorized Access, Man-in-the-Middle, Session Hijacking, and Replay. Furthermore, Sachin Babar et al. [69] undertook a classification of threats motivated by IoT security requirements. These encompassed crucial facets such as identification, communication, physical threat, embedded security, and storage management. This nuanced approach serves to enhance our understanding of threat landscapes within the context of evolving security paradigms.

Verkerken et al. [70] used the CIC-IDS-2017 NIDS dataset to assess the effectiveness of several unsupervised machine learning models. The study emphasizes how crucial unsupervised methods are for identifying zero-day attack groups. To reduce the dimensionality of the dataset, PCA is used for transformation. The models in a one-class classification technique were assessed on combined (benign and malicious) data samples after being trained on benign-only data sets. Autoencoders produce the highest detection performance, with a 96.16% F1 score, according to the data. One-class SVM, isolated forest, and PCA classifiers follow after. Liu and Zhang [71] proposed an intrusion detection model that cleverly integrates the strengths of both signature-based recognition and immune-based recognition methods. Their approach involved defining

numerical data features specifically tailored for intrusion detection, coupled with the implementation of a subfeature-based numerical matching method to enhance precision. The model's performance was evaluated using the KDD Cup 99 dataset, where it exhibited an impressive detection rate of 90.706%.

In their study [72], the author introduced an innovative intrusion detection scheme that leverages a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) approach. This scheme is specifically designed for detecting network anomalies with a focus on accuracy. Notably, the research is conducted in a centralized manner, highlighting the potential for effective detection and management of network intrusions. The integration of CNN and LSTM techniques underscores the commitment to advancing intrusion detection.

The author in [73] advocates for the adoption of a decentralized intrusion detection scheme employing federated learning methodologies. The proposed scheme strategically avoids centralizing datasets, opting instead for a distributed setting where models operate collaboratively across multiple locations. Notably, through meticulous implementation, the author achieved a commendable accuracy of 88.92%.

2.3 Summary

In light of existing traditional threat taxonomies, a pressing demand has surfaced for a contemporary and adaptable framework, prompted by the pervasive nature of common attacks within present-day Intrusion Detection System (IDS). The absence of a modern cyber threat taxonomy not only poses a challenge but also hinders researchers in effectively gauging the threat coverage. Addressing this gap, the development of a generic and modular taxonomy for security threats emerges as a crucial initiative. Such a taxonomy not only aids researchers but also empowers cybersecurity practitioners to construct tools with enhanced capabilities, capable of identifying a comprehensive spectrum of attacks, spanning known, advanced, and emerging zero-day threats.

The predominant paradigm in intrusion detection involves centralized techniques, presenting inherent vulnerabilities associated with data breach risks. The conventional methodology necessitates the aggregation of extensive datasets for training Intrusion Detection Systems (IDS). In response to this challenge, an alternative approach is posited,

emphasizing a decentralized framework leveraging federated learning. This approach aims to mitigate the risk of data leakage by distributing the training process across diverse nodes. In the current research, we propose an innovative decentralized strategy, complemented by the incorporation of differential privacy (DP) as a privacy enhancement technique. The choice of a decentralized framework not only addresses concerns related to data confidentiality but also fosters collaborative learning without the need for centralized data repositories. The upcoming chapter provides a thorough exploration of the nuanced aspects inherent in both the proposed framework and the concept of differential privacy, offering a comprehensive analysis of their functions. This research endeavors to contribute to the advancement of privacy-aware intrusion detection methodologies.

Methodology

In the preceding chapter, we delved into the diverse landscape of intrusion detection systems, exploring the multifaceted realm of cybersecurity solutions designed to safeguard against unauthorized access and potential threats. Building upon this foundational understanding, the ensuing chapter embarks on an exploration of our decentralized approach.

3.1 Framework

This section describes our proposed framework for decentralized collaborative intrusion detection system. Figure 3.1 show the proposed framework. The foundational philosophy is encapsulated by federated learning (FL). At its core, FL endeavors to derive a model based on the data residing autonomously at individual clients. This is different from conventional machine learning (ML) paradigms, where large datasets are traditionally aggregated at a central location, thereby introducing an inherent susceptibility to security breaches. In contrast, FL operates on a principle wherein each client retains possession of its respective data. This decentralized architecture aligns with contemporary privacy considerations. The inherent advantage of this approach lies in its ability to circumvent the risks posed by a centralized data repository, thereby enhancing the security posture of the intrusion detection system. Embedded within our framework, this FL-based methodology further contributes to the preservation of data privacy, as training occurs locally on each client without necessitating the transmission of raw data to a central server. The amalgamation of federated learning and differential privacy (Pri-

vacy enhancement technique) within our proposed approach establishes a resilient and secure foundation for decentralized intrusion detection, thereby advancing the discourse on innovative strategies within the realm of cybersecurity

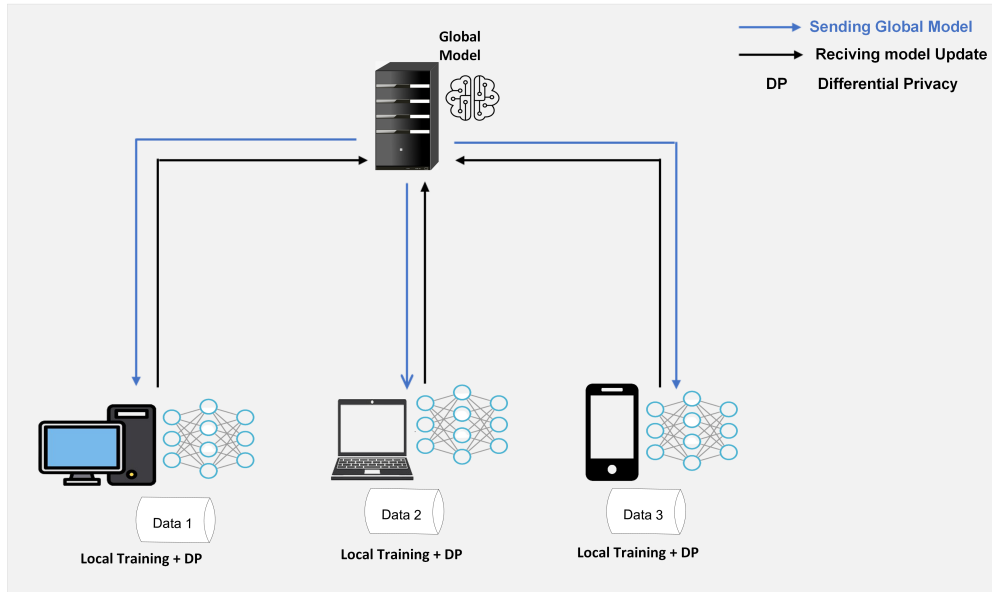


Figure 3.1: The Framework for privacy aware decentralized intrusion detection system

3.2 Data Extraction and Preprocessing

3.2.1 Data Extraction

The dataset for this study is acquired from the cyber range lab of the Australian Centre for Cyber Security (ACCS) at University of New South Wales (UNSW) in Canberra. The synthesis of the dataset involved using the IXIA PerfectStorm tool, allowing for the creation of a comprehensive dataset that includes both benign network activities from testbed scenarios and synthetic attack scenarios. The data collection was carried out with the tcpdump tool, resulting in capturing a substantial dataset of 100 GB in pcap files. Following data acquisition, a set of tools, including Argus, Bro-IDS, and twelve additional SQL algorithms, were utilized to carefully extract relevant features from the dataset. The dataset consists of a total of two million and 540,044 records distributed across four CSV files. A portion of this dataset was specifically allocated for training and testing purposes, referred to as the training set and testing set, with 175,341 records and 82,332 records, respectively. [74–77].

3.2.2 Data preprocessing

A thorough and systematic strategy was taken in order to ensure the integrity and analytical viability of the data when it came to preprocessing the UNSW-NB15 dataset. The data preprocessing process is described in Figure 3.1 In order to enable specific processing strategies, the first stage involved the separation of numerical and categorical data features. Then, in order to guarantee a complete dataset, missing values in the dataset were imputed. The numerical characteristics were then normalized using feature scaling, which helped to homogenize the data distributions. Finally, a careful feature selection procedure was carried out with the goal of reducing the dataset to its most important characteristics in order to maximize computing effectiveness and improve the interpretability of further analyses.

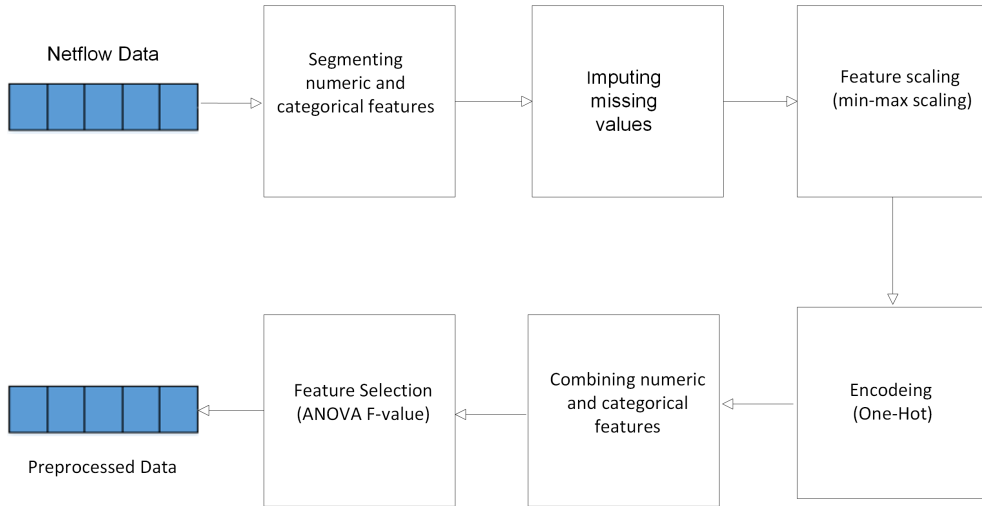


Figure 3.2: Data preprocessing workflow

3.3 Model Initialization

After the local preprocessing of data on each client, a Deep Neural Network (DNN) model is globally initialized. Subsequently, this model is broadcasted to each participating client. In our decentralized approach, as opposed to the conventional practice of aggregating data at a centralized location, the model is dispatched to individual clients, each possessing its own data. This decentralization preserves the privacy of sensitive data, as the model traverses to the data, mitigating the need for central data collection. Upon reaching each client, the model undergoes localized training for a specified number

of epochs. Post-training, it returns to the central server after the application of differential privacy mechanisms to the model weights. This strategic integration of differential privacy ensures that individual client data remains secure, preventing unauthorized decoding during model transmission. The differentially private models are subsequently aggregated at the central server, marking the completion of one learning round.

For subsequent iterations, the aggregated model, now imbued with the knowledge acquired from individual clients, serves as the starting point. This iterative process of model distribution, local training, and aggregation continues, each round building upon the insights gained from the decentralized training paradigm. Throughout these iterations, the performance metrics of the model are meticulously calculated, providing a comprehensive evaluation of its efficacy and adaptability within the decentralized learning framework. This methodology, rooted in privacy-preserving practices and iterative model refinement, epitomizes the innovative potential of decentralized learning paradigms in contemporary data-centric applications.

DNN Classifier

We proposed a Deep neural network (DNN) classifier for intrusion detection. DNN is a type of artificial neural network with multiple layers between the input and output layers. It excels in learning intricate patterns and representations from complex data, enabling it to tackle sophisticated tasks. DNNs leverage deep learning techniques to automatically extract hierarchical features, making them powerful tools in various machine learning applications.

In this methodology, Deep Neural Network (DNN) models undergo collaborative training across a network of diverse devices or clients, without necessitating the direct exchange of raw data. This decentralized training paradigm ensures the preservation of privacy and security by confining sensitive information to local environments, while concurrently leveraging collective learning across the network to augment the capabilities of intrusion detection. The resulting decentralized training process contributes to the establishment of a resilient and adaptive defense mechanism against the continually evolving landscape of cyber threats. This approach facilitates the synthesis of diverse insights from disparate sources, enhancing the robustness of the intrusion detection system through a federated learning framework.

The preprocessed data is fed into the input layer of the neural network. The data

then propagates through the hidden layers, where the neural network learns to extract intricate patterns and representations relevant to distinguishing between normal and malicious network behavior. These hidden layers are designed to capture hierarchical features in the data, enabling the network to make informed decisions about potential network intrusions based on the learned patterns. After each hidden layer, a Rectified Linear Unit (ReLU) activation function is employed. This activation function, expressed by the equation 3.3.1 introduces non-linearity to the network, thereby improving its capacity to discern intricate patterns and relationships within the data.

$$f(x) = \max(0, x) \quad (3.3.1)$$

The ReLU also helps in the generalization ability of the DNNs model and also reduces the computational cost of the model.

Binary Cross-Entropy, also known as log loss or logistic loss, is used as a loss function. It measures the dissimilarity between the predicted probability distribution and the actual labels. The goal during training is to minimize this loss, guiding the model to make predictions that align with the true labels.

$$L = -\frac{1}{N} \sum_{i=1}^N (y_i \cdot \log(p_i) + (1 - y_i) \cdot \log(1 - p_i)) \quad (3.3.2)$$

The equation penalizes the model more if the predicted probability diverges from the true label.

3.4 Privacy Preserving

Various privacy enhancement schemes are employed to safeguard individuals' sensitive information within datasets. Anonymization or de-identification is one such approach, involving the removal of any data elements that could identify an individual. Encryption, while offering robust privacy protection, poses challenges for statistical analysis on encrypted data, necessitating specialized methods. Despite the advantages of encryption in providing privacy to individuals and enabling third-party analytics, the significant computational overhead required for such operations is a notable limitation. Moreover, the dynamic landscape of privacy preservation continually introduces innovative

techniques, each with its trade-offs. Achieving a harmonious balance between ensuring individual privacy and addressing the practical challenges of computation-intensive methods is imperative for the effective deployment of privacy-enhancing mechanisms in diverse data-driven domains. Given these considerations, differential privacy emerges as a prominent approach for ensuring data privacy. Differential privacy [78] aims to protect individual privacy while allowing for meaningful data analysis, striking a balance between privacy preservation and data utility.

Differential Privacy:

Differential privacy [78, 79] offers a sophisticated and stringent mathematical method for determining an amount of privacy guaranteed by a privacy-preserving system [80, 81]. Statistically indistinguishable outcomes will be produced by a differentially private privacy-preserving process operating on similar datasets. In the context of ϵ -differential privacy, the main objective is the construction of a resilient framework that ensures privacy throughout transitions between closely related datasets. The goal is contingent upon the stability of the probability of observing a specific outcome (ξ) within the purview of a randomized algorithmic function ϕ , especially when datasets β and β' undergo an adjacent transition:

$$|P(\phi(\beta) = \xi) - P(\phi(\beta') = \xi)| \leq e^\epsilon \cdot P(\phi(\beta') = \xi) \quad (3.4.1)$$

Here, the epsilon parameter (ϵ) assumes a pivotal role, delineating the degree of privacy conferred by the mechanism. A lower ϵ conveys a more robust privacy assurance, elucidating the delicate trade-off inherent in privacy-preserving mechanisms.

The incorporation of the differential privacy function ϕ into the randomized algorithm A is succinctly expressed as:

$$A(\beta) = \phi(\beta) + \text{Lap}(\delta_{fs}/\epsilon) \quad (3.4.2)$$

In this equation, A symbolizes the randomized algorithm, $\phi(\beta)$ represents the application of the differential privacy function to dataset β , and $\text{Lap}(\frac{\delta_{fs}}{\epsilon})$ introduces Laplace noise following the Laplace distribution with a scale parameter of $\frac{\delta_{fs}}{\epsilon}$. This mechanism rigorously adheres to the ϵ -differential privacy parameter, strategically utilizing Laplace

noise for privacy preservation.

The Laplace mechanism, an indispensable component, introduces controlled perturbations through Laplacian noise to each coordinate of the data. Governed by the sensitivity of the differential privacy function $\frac{\delta_{fs}}{\epsilon}$, this approach proves particularly effective in scenarios involving numerical output results.

Additionally, the Laplace noise conforms to the Laplace distribution, characterized by the probability density function:

$$f(x; \mu, b) = \frac{1}{2b} \exp\left(-\frac{|x - \mu|}{b}\right) \quad (3.4.3)$$

This distribution, renowned for its heavier tails, introduces a deliberate level of controlled randomness, enhancing privacy preservation while concurrently safeguarding the utility of the underlying data. The ϵ -differential privacy framework adeptly navigates the intricate terrain of privacy preservation, demonstrating a judicious balance between privacy assurance and data utility.

3.5 Model Aggregation

In this decentralized paradigm of federated learning, the aggregation stage plays a crucial role in coordinating the iterative combination of model weights. This iterative combination occurs when locally trained model parameters from each client go to the central server, where a aggregation technique is systematically implemented. The iterative nature of this aggregation not only accommodates the dynamic evolution of decentralized data distributions among clients but also guides the federated learning system towards the convergence of an optimally refined global model. This iterative structure serves as a strategic nexus, connecting the inherent variability associated with localized training methodologies to the key objective of cultivating a unified, privacy-aware global model.

In this study, three different model aggregation strategies, FedAvg (Federated Averaging), FedAdam (Federated Adam), and FedAdagrad (Federated Adaptive Gradient), are used. The comprehensive exploration of these aggregation mechanisms, detailed in the subsequent chapter. FedAvg, a methodology characterized by the collaborative averaging of model parameters across diverse clients, is instrumental in fostering a col-

lective learning environment. In contrast, FedAdam dynamically adapts the aggregation process to disparate historical gradients through the incorporation of adaptive learning rates derived from the Adam optimization method. Further enhancing the diversity of approaches, FedAdagrad incorporates individualized learning rates for each parameter, thereby promoting an effective fusion of models that accounts for nuanced variations in data distributions. This meticulous examination of model aggregation mechanisms contributes to a deeper comprehension of their nuanced dynamics within the complex fabric of decentralized learning environment.

Results and Discussion

This chapter presents the experimental findings of our intrusion detection solution, focusing on the evaluation of its efficacy. Through rigorous testing featuring diverse network configurations and simulated threats, the system's performance is assessed using key metrics such as accuracy, true positive rate (TPR), and F1 score. The results illuminate the solution's ability to accurately identify and classify security threats, offering insights into its practical utility. Comparative analyses against centralized, decentralized and decentralized with Privacy Enhancement Techniques (PET) are also discussed.

4.1 Centralized Approach

In the initial phase of the study, a centralized approach was employed for the intrusion detection system (IDS). This methodology involved the consolidation of the entire dataset onto a central repository, serving as a unified data hub for subsequent analyses. The rationale behind this centralized framework was to systematically orchestrate experiments and assessments in a controlled and homogeneous environment. The consolidated dataset facilitated comprehensive evaluations of the IDS performance, enabling a thorough examination of its efficacy in identifying and mitigating potential security breaches. Experimental scenarios, encompassing diverse network configurations and simulated intrusion instances, were systematically conducted within this centralized paradigm to ascertain the system's response under varying conditions. The centralized data repository served as a pivotal element in standardizing experimental conditions, thereby providing a foundational basis for subsequent comparative analyses and assessments of the

intrusion detection system.

Outcomes of Centralized Approach:

In the initial phase of our investigation, a centralized approach was adopted for the intrusion detection system (IDS). This methodology involved the consolidation of the entire dataset onto a singular repository, providing a centralized locus for subsequent analyses. The centralized approach aims to streamline and standardize the experimental environment, ensuring a homogenous basis for evaluating the intrusion detection system’s performance under controlled conditions.

Parameters	Values
Learning rate	0.01
Batch size	64
Number of epochs	20
Optimizer	Adam
Momentum	0.5

Table 4.1: Model Training Parameters for Centralised Approach

The primary training parameters used in the Deep Neural Network (DNN) for the intrusion detection task are shown in Table 4.1. The DNN’s training dynamics are carefully optimized by adjusting these parameters, which include learning rate, batch size, optimization algorithm, and number of epochs. Table 4.1 provides a systematic presentation that is an essential point of reference. The results obtained from the centralized approach are depicted in Figure 4.1. The centralized scenario produced impressive results, displaying a TPR of 99.5% and other associated metrics.

4.2 Decentralized Without PET

In the decentralized paradigm, each participating entity, denoted as a client, possesses a distinct dataset exclusive to its domain. This configuration necessitates the establishment of a global model, which is systematically disseminated to each individual client in the network. Upon reception of the global model, each client embarks on local model

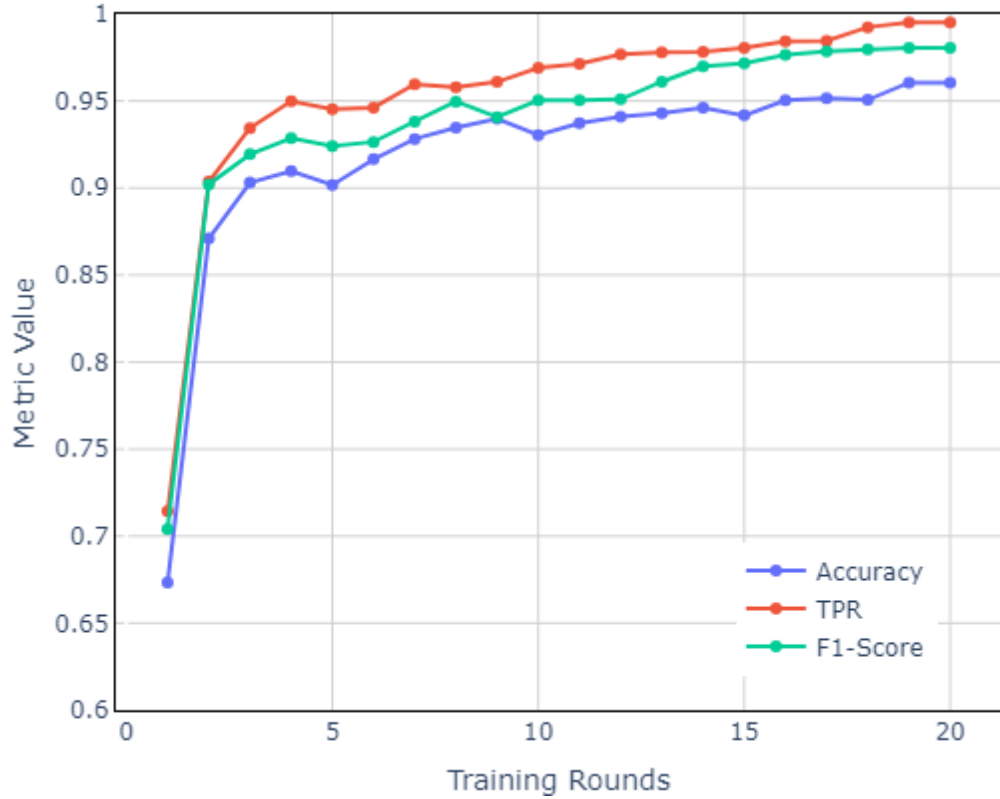


Figure 4.1: Model Performance in Centralized Scenario

training, leveraging its unique dataset. The localized training process is characterized by the autonomous processing of data within the confines of each client’s domain. Subsequently, the locally trained models are offloaded and transmitted to a central server, where they undergo a process of aggregation.

The aggregation process, situated at the central server, involves the synthesis of locally trained models from each participating client. Employing methodologies such as federated averaging, the central server amalgamates the diverse insights and updates contributed by individual clients. This iterative federated learning process unfolds in a systematic manner, enabling the continual refinement of the global model.

Outcomes of Decentralized with out PET:

In the decentralized framework adopted for this study, individual client entities assume custodianship of their respective datasets. However, it is noteworthy that the current implementation lacks the incorporation of Privacy Enhancement Techniques (The Differential Privacy is used as a PET as discussed in next section). This absence of PET introduces considerations regarding the privacy and security aspects of the decentralized

data distribution model. The parameters governing the Deep Neural Network (DNN) utilized in this decentralized context are meticulously configured and documented in Table 4.2, providing transparency and reproducibility in the experimental setup.

Parameters	Values
Learning rate	0.01
Batch size	64
Number of epochs (local)	5
Number of learn- ing rounds	20
Optimizer	Adam
Momentum	0.5

Table 4.2: Model Training Parameters for decentralised Approach

Concurrently, the empirical outcomes of the decentralized approach are visually presented and critically analyzed in Figure 4.2. the True Positive Rate (TPR) for the decentralized approach is reported at 98%, a metric that is marginally lower than its centralized counterpart. It is imperative to note that, in the absence of Privacy Enhancement Techniques, the data privacy implications and potential vulnerabilities warrant comprehensive scrutiny.

4.3 Decentralized with PET

In the preceding section, our experimentation was conducted within a decentralized paradigm, devoid of a designated privacy enhancement scheme. Subsequently, in an effort to fortify the security of the distributed data, we introduce Differential Privacy (DP) as a pivotal privacy enhancement scheme. The objective is to mitigate potential privacy risks associated with data transmission, particularly in scenarios where eavesdropping on the network might compromise confidentiality.

The distribution of data to diverse clients, while conducive to collaborative model train-

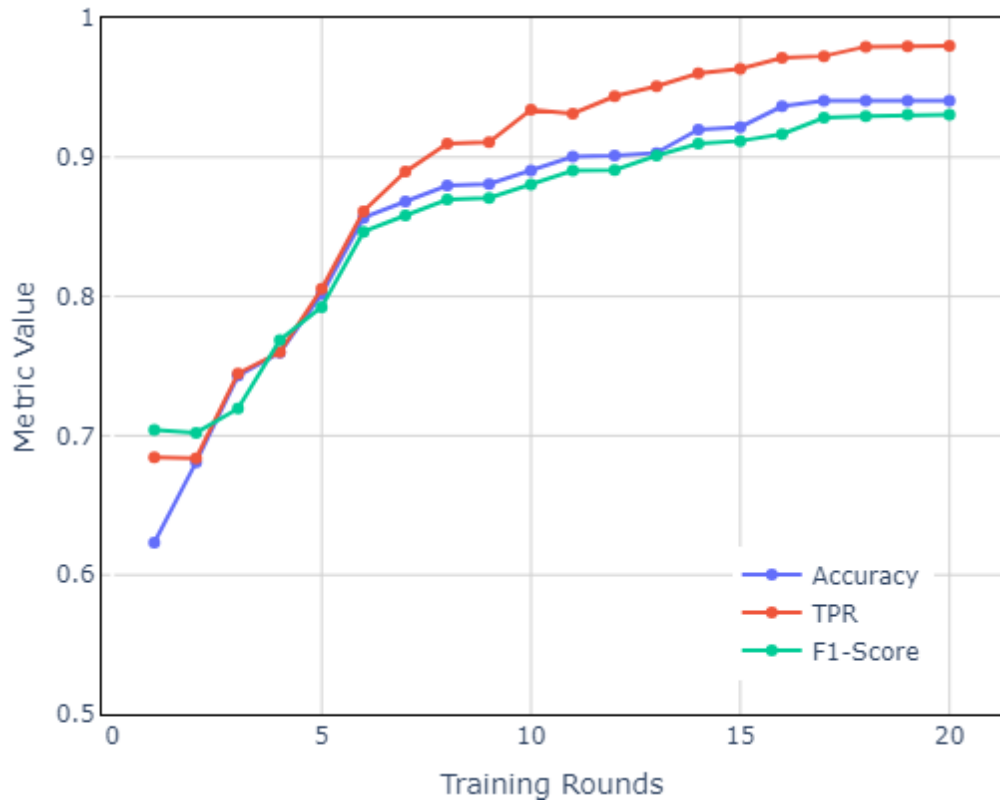


Figure 4.2: Model Performance for Decentralized Approach without PET

ing, may introduces security concerns. In the absence of privacy measures, there exists the possibility of data interception by malicious entities. To address this vulnerability, Differential Privacy is strategically employed. This scheme, as comprehensively discussed in the preceding chapter, serves as a robust protective mechanism for the sensitive and confidential data hosted by each participating client.

The procedural workflow involves the initiation of a global model, with its parameters meticulously configured, a detail elucidated in Table 4.2. This global model is then disseminated to the participating clients, where each client undertakes local model training. The incorporation of Differential Privacy at this stage ensures that the training process is attuned to preserving the privacy of individual client datasets.

Subsequently, the locally trained models, imbued with the protective cloak of Differential Privacy, are transmitted back to the central server. At this juncture, the amalgamation of these differentially private models is performed through an aggregation process. Notably, this step is pivotal, as it serves as the crux for deriving collective insights from individual client contributions while upholding privacy constraints.

In this scenario we consider three different aggregation schemes namely FedAvg (Federated Averaging), FedAdam (Federated Adam), and FedAdagrad (Federated Adaptive Gradient).

4.3.1 FedAvg (Federated Averaging)

FedAvg stands as a foundational Federated Learning (FL) technique, orchestrating the cooperative training of a global model by aggregating local model updates from a diverse array of clients. This collaborative aggregation process is pivotal, encapsulating a unified representation of distributed learning across the network. It acts as a linchpin, providing a cohesive and harmonized foundation for subsequent training iterations [82].

The Figure 4.3, presents the depiction of the performance outcomes associated with the FedAvg federated learning approach.

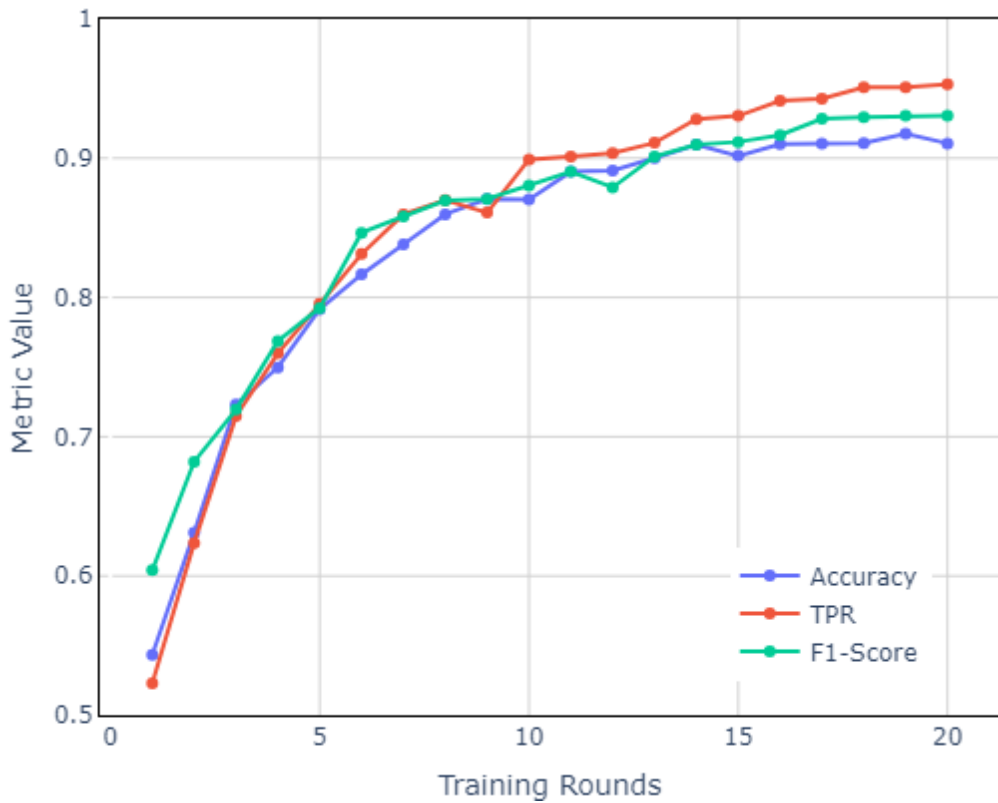


Figure 4.3: Results with FedAvg Aggregation Mechanism.

4.3.2 FedAdam (Federated Adam)

FedAdam stands as a prominent algorithm within the Federated Learning landscape, seamlessly incorporating the advantageous features of the Adam optimizer into the federated learning paradigm. Noteworthy for its utilization of adaptive learning rates and momentum, FedAdam blends the proficient updating of the global model by assimilating local updates contributed by individual clients. This distinctive process involves the aggregation of gradients computed locally on various devices, culminating at a central server. The aggregation, often implemented through algorithms like weighted averaging, yields an approximated global gradient. FedAdam represents an intricate amalgamation of Adam's optimization prowess with the collaborative Federated Learning framework, thereby facilitating heightened efficiency and improved model performance [83].

In Figure 4.4, the results corresponding to this scenario are visually presented, offering a comprehensive illustration of the performance outcomes associated with FedAdam in the federated learning context.

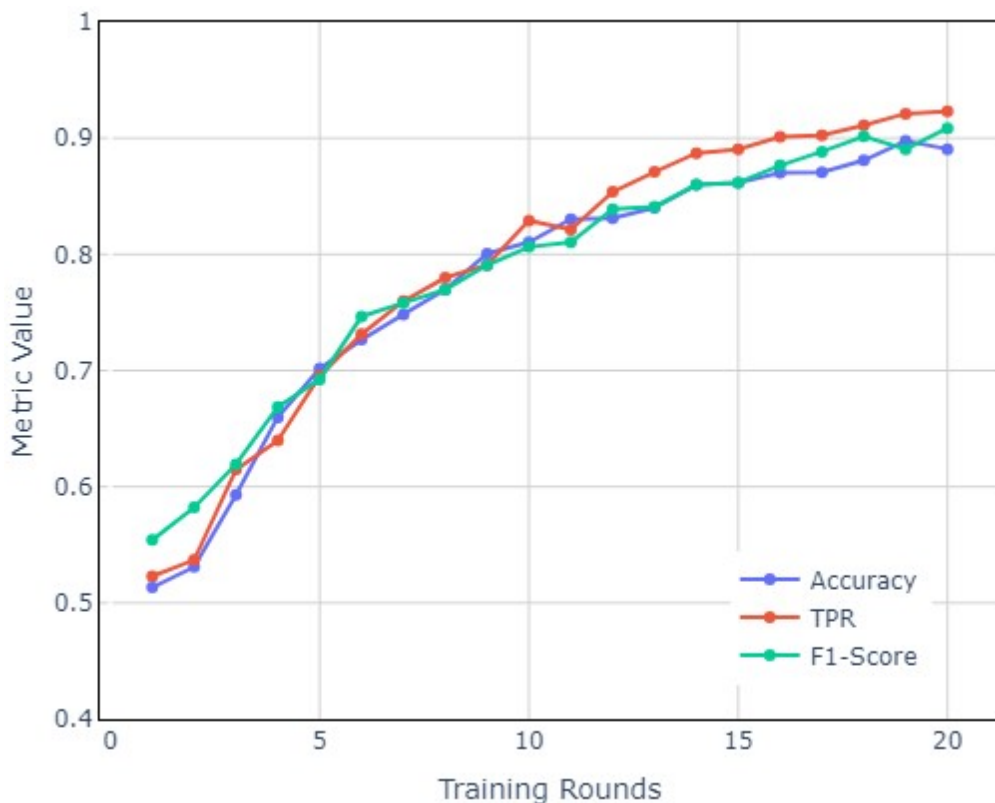


Figure 4.4: Results with FedAdam Aggregation Mechanism.

4.3.3 FedAdagrad (Federated Adaptive Gradient)

FedAdagrad, a refined iteration within the Federated Learning paradigm, integrates the dynamic optimization technique of Adagrad into its framework. This modification demonstrates a sophisticated approach by intelligently adjusting the learning rates for specific model parameters based on their historical gradients. This adaptive mechanism significantly expedites model convergence, resulting in an enhanced overall performance. In contrast to conventional methods reliant on parameter averaging, FedAdagrad places emphasis on gradient aggregation, a characteristic that contributes to its nuanced and accelerated training dynamics [83]. The learning curves corresponding to this scenario are visually represented in 4.5.

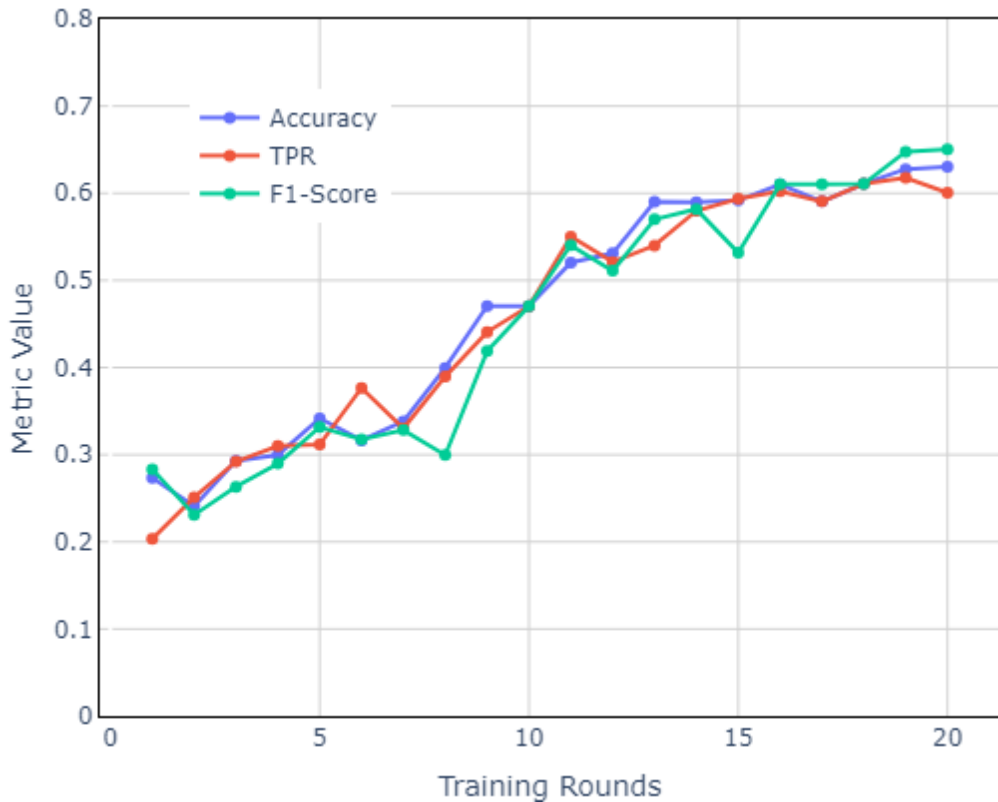


Figure 4.5: Results with FedAdagrad Aggregation Mechanism.

The implications of employing diverse aggregation mechanisms on the overall model performance are graphically illustrated in Figures 4.3, 4.4 and 4.5, respectively. In this specific use case, FedAvg emerges as the most favorable approach, yielding highly promising outcomes. It achieves a commendable True Positive Rate (TPR) of 95%, indicating its efficacy in correctly identifying positive instances. Following closely are FedAdam and FedAdagrad, showcasing their comparative performances within the federated learning

framework.

FedAvg’s superior performance can be attributed to its methodology of federated averaging, where model updates from various clients are collectively averaged, fostering a collaborative and coherent global model. This collaborative approach ensures a robust and accurate representation of the overall dataset, contributing to the heightened TPR observed.

While FedAdam and FedAdagrad demonstrate competitive performances, their nuanced differences stem from the optimization techniques they incorporate. FedAdam leverages adaptive learning rates and momentum from the Adam optimizer, combining optimization efficiency with federated learning dynamics. On the other hand, FedAdagrad employs the Adagrad dynamic optimization technique, intelligently adjusting learning rates based on historical gradients.

4.4 Comparison

In this section the comparison among three different schemes centralized, decentralized with out PET and decentralized with DP is presented.

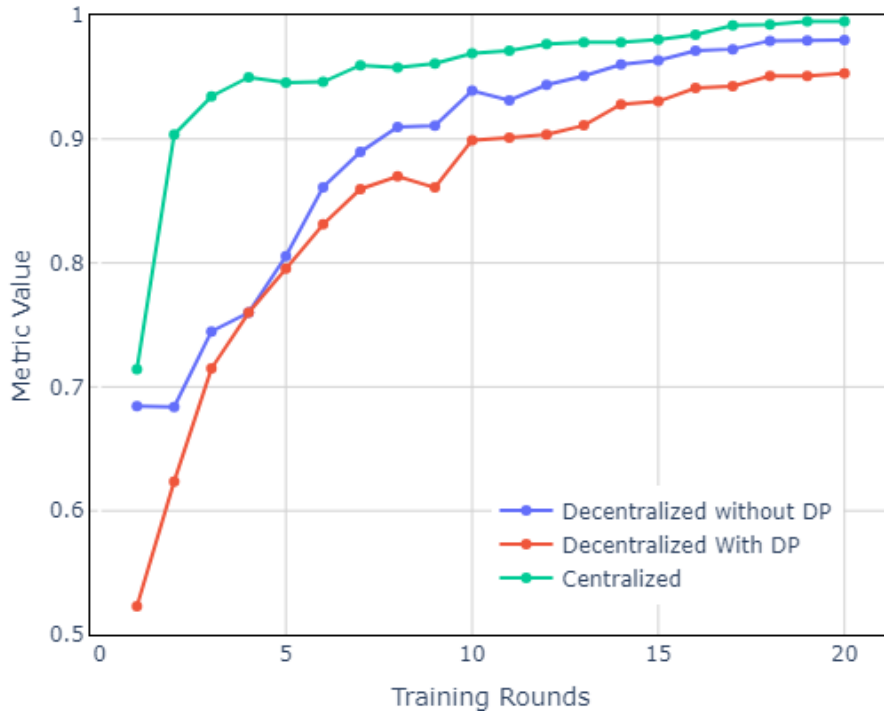


Figure 4.6: Comparison of Results in different settings

After a thorough set of experiments, it became evident that there is a delicate tradeoff between privacy and utility. The augmentation of privacy was observed to inversely impact the model’s utility, and vice versa. Consequently, experiments varying the values of epsilon were conducted, revealing a notable equilibrium between privacy and utility, as depicted in Figure 4.3.

Figure 4.6 provides a comparative analysis among centralized, decentralized, and decentralized with PET configurations. Despite the seemingly diminished results with PET, it is imperative to underscore that they reflect heightened privacy awareness.

We established the centralized model as the benchmark to conduct a rigorous evaluation of a decentralized framework’s performance. Through systematic experimentation, we explored two distinct decentralized scenarios (as discussed above): one without the incorporation of differential privacy and other integrating differential privacy as privacy enhancement technique. The aim was to identify subtle differences in the model’s performance in relation to the standard benchmark, which was the centralized method. This evaluation included the calculation of both the mean absolute difference (MAD) as shown in Figure 4.7 and mean squared difference (MSD) as shown in Figure 4.8 to provide a quantitative assessment of the observed deviations.

The values obtained for Mean Squared Difference (MSD) were 0.0082001 without DP and 0.0148552 with DP, highlighting a minute difference in model performance between the two scenarios. The figure 4.8 visually depict this subtle distinction. Despite this performance difference, the incorporation of DP significantly enhances privacy measures, reinforcing the importance of its integration in decentralized frameworks. These findings provide a comprehensive understanding of the trade-off between minute performance distinctions and the heightened privacy afforded by DP within the context of decentralized network intrusion detection systems.

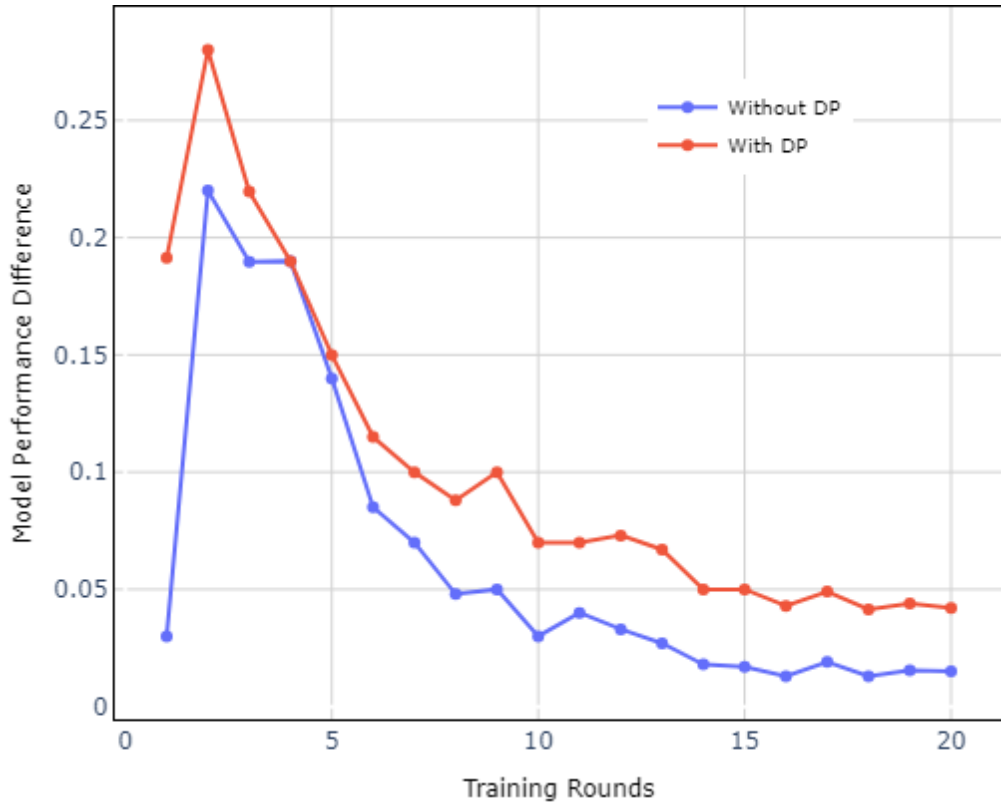


Figure 4.7: MAD of decentralized approach with respect to centralized

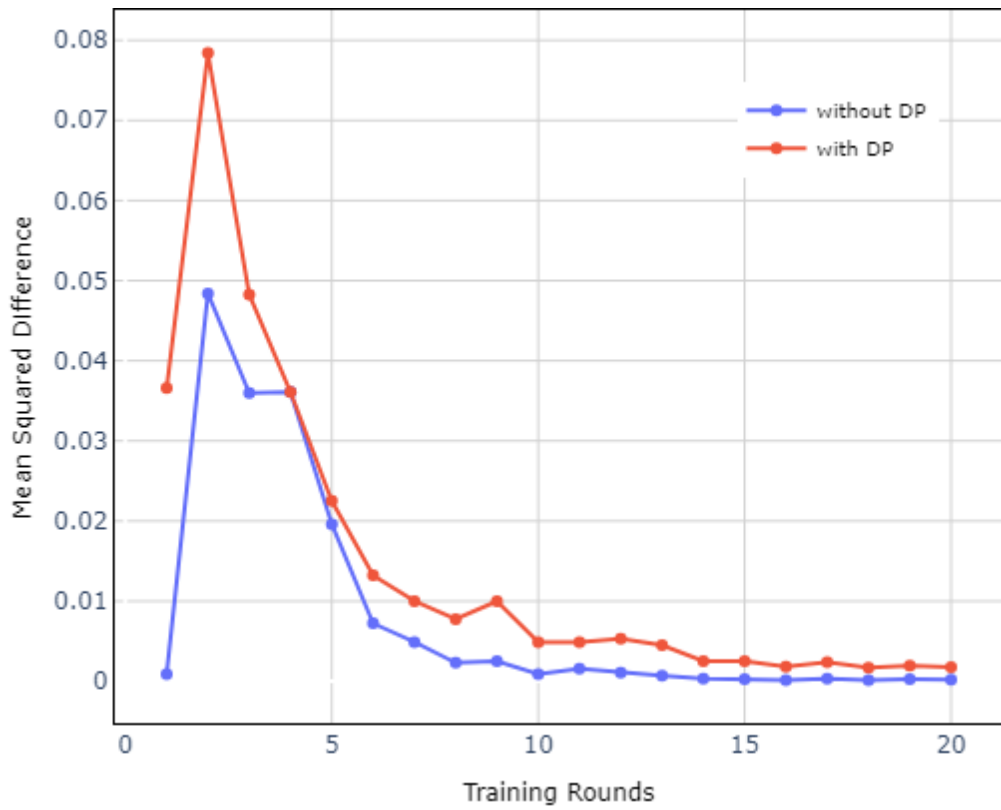


Figure 4.8: MSD of decentralized approach with respect to centralized

Conclusion and Recommendation

5.1 Conclusion

IDS are tools that oversee and examine network traffic to detect anomalies and cyber threats. Different ML approaches have been suggested in the past decade to build IDS. The work presented in this study aims the use of decentralized ML techniques to build IDS. This study entailed the systematic development of a decentralized intrusion detection framework utilizing Netflow data obtained from UNSW. A Deep Neural Network (DNN) five local training epochs, and twenty rounds of Federated Learning (FL) was deployed inside the recommended design framework in order to identify the complex patterns present in the network data. The design's meticulous construction and rigorous testing underscore its potential contribution to the evolving cybersecurity landscape. This investigation not only highlights the commendable efficacy of Federated Learning but also clarifies its pivotal role in cultivating a secure and privacy-conscious network environment. Three distinct settings were carefully considered for the experiments: centralized, decentralized, and decentralized with the thoughtful addition of differential privacy. A remarkable 99.51% True Positive Rate (TPR) were attained in the centralized technique. On the other hand, a TPR of 98.05% was noted in the decentralized case where no Privacy Enhancement Techniques (PET) were used, and TPR of 95.31% was achieved in the decentralized scenario with differential privacy. When analyzing the results under various scenarios, it is important to notice that the decentralized method combined with differential privacy produces somewhat marginal reduction in performance outcomes. The Mean Squared Difference (MSD) values, when calculated

against the centralized benchmark, reveal a minute difference. The values obtained for Mean Squared Difference (MSD) were 0.0082001 without DP and 0.0148552 with DP, highlighting a minute difference in model performance between the two scenarios when compared to the conventional centralized approach. It is crucial to emphasize, nonetheless, that this slight drop in performance measurements is a responsible compromise for the increased security guarantees and privacy-aware environment that come with this methodology. This delicate balance highlights how important it is to put a privacy-aware framework first when building stronger network protection models. The suggested approach contribute to the field of network security by offering a reliable and effective way to detect security risks.

5.2 Recommendations

As a recommendation for future work, it is suggested to enhance the proposed solution by addressing additional security vulnerabilities beyond network intrusions. Furthermore, exploring various aggregation schemes and studying the synchronization of model updates from different nodes could provide valuable insights for further improvement. Lastly, testing the approach proposed in this thesis in a real-life testing environment may yield more insights. As opposed to benchmark dataset assessment, this will further highlight the demands and requirements in various operational settings.

References

- [1] Ioannis Stelios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 20(4):3453–3495, 2018.
- [2] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. Internet of things (iot): Taxonomy of security attacks. In *2016 3rd international conference on electronic design (ICED)*, pages 321–326. IEEE, 2016.
- [3] Md Haris Uddin Sharif and Mehmood Ali Mohammed. A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, 15(1):138–156, 2022.
- [4] Brian Cashell, William D Jackson, Mark Jickling, and Baird Webel. The economic impact of cyber-attacks. *Congressional research service documents, CRS RL32331 (Washington DC)*, 2, 2004.
- [5] Aaron Zimba and Mumbi Chishimba. On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research*, 4(1):3–31, 2019.
- [6] David Tipper. Resilient network design: challenges and future directions. *Telecommunication Systems*, 56:5–16, 2014.
- [7] Kash Barker, James H Lambert, Christopher W Zobel, Andrea H Tapia, Jose E Ramirez-Marquez, Laura Albert, Charles D Nicholson, and Cornelia Caragea. Defining resilience analytics for interdependent cyber-physical-social networks. *Sustainable and Resilient Infrastructure*, 2(2):59–67, 2017.

REFERENCES

- [8] Biswanath Mukherjee, L Todd Heberlein, and Karl N Levitt. Network intrusion detection. *IEEE network*, 8(3):26–41, 1994.
- [9] Sattarova Feruza Yusufvna. Integrating intrusion detection system and data mining. In *2008 International Symposium on Ubiquitous Multimedia Computing*, pages 256–259. IEEE, 2008.
- [10] Chirag N Modi, Dhiren R Patel, Avi Patel, and Rajarajan Muttukrishnan. Bayesian classifier and snort based network intrusion detection system in cloud computing. In *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, pages 1–7. IEEE, 2012.
- [11] Moses Garuba, Chunmei Liu, and Duane Fraites. Intrusion techniques: Comparative study of network intrusion detection systems. In *Fifth International Conference on Information Technology: New Generations (itng 2008)*, pages 592–598. IEEE, 2008.
- [12] Vinod Kumar and Om Prakash Sangwan. Signature based intrusion detection system using snort. *International Journal of Computer Applications & Information Technology*, 1(3):35–41, 2012.
- [13] Payam Vahdani Amoli, Timo Hamalainen, Gil David, Mikhail Zolotukhin, and Mahsa Mirzamohammad. Unsupervised network intrusion detection systems for zero-day fast-spreading attacks and botnets. *JDCTA (International Journal of Digital Content Technology and its Applications)*, 10(2):1–13, 2016.
- [14] Pedro Garcia-Teodoro, Jesus Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, 28(1-2):18–28, 2009.
- [15] Parth Bhatt, Edgar Toshiro Yano, and Per Gustavsson. Towards a framework to detect multi-stage advanced persistent threats attacks. In *2014 IEEE 8th international symposium on service oriented system engineering*, pages 390–395. IEEE, 2014.
- [16] VVRPV Jyothisna, Rama Prasad, and K Munivara Prasad. A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, 28(7):26–35, 2011.

- [17] Zoubin Ghahramani. Probabilistic machine learning and artificial intelligence. *Nature*, 521(7553):452–459, 2015.
- [18] Trishan Panch, Peter Szolovits, and Rifat Atun. Artificial intelligence, machine learning and health systems. *Journal of global health*, 8(2), 2018.
- [19] John R Koza, Forrest H Bennett, David Andre, and Martin A Keane. Automated design of both the topology and sizing of analog electrical circuits using genetic programming. *Artificial intelligence in design'96*, pages 151–170, 1996.
- [20] Maryam M Najafabadi, Flavio Villanustre, Taghi M Khoshgoftaar, Naeem Seliya, Randall Wald, and Edin Muharemagic. Deep learning applications and challenges in big data analytics. *Journal of big data*, 2(1):1–21, 2015.
- [21] Robin Bloomfield, Heidy Khlaaf, Philippa Ryan Conmy, and Gareth Fletcher. Disruptive innovations and disruptive assurance: Assuring machine learning and autonomy. *Computer*, 52(9):82–89, 2019.
- [22] Michael I Jordan and Tom M Mitchell. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245):255–260, 2015.
- [23] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Intrusion detection by machine learning: A review. *expert systems with applications*, 36(10):11994–12000, 2009.
- [24] Hongyu Liu and Bo Lang. Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, 9(20):4396, 2019.
- [25] Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419, 2020.
- [26] Yong Zhang, Xu Chen, Lei Jin, Xiaojuan Wang, and Da Guo. Network intrusion detection: Based on deep hierarchical network and original flow data. *IEEE Access*, 7:37004–37016, 2019.
- [27] Ming Liu, Zhi Xue, Xianghua Xu, Changmin Zhong, and Jinjun Chen. Host-based intrusion detection system with system calls: Review and future trends. *ACM Computing Surveys (CSUR)*, 51(5):1–36, 2018.

REFERENCES

- [28] Mohammad Masdari and Hemn Khezri. A survey and taxonomy of the fuzzy signature-based intrusion detection systems. *Applied Soft Computing*, 92:106301, 2020.
- [29] Wei Wang, Yiqiang Sheng, Jinlin Wang, Xuwen Zeng, Xiaozhou Ye, Yongzhong Huang, and Ming Zhu. Hast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE access*, 6:1792–1806, 2017.
- [30] Simon D Duque Anton and Hans D Schotten. Intrusion detection in binary process data: introducing the hamming-distance to matrix profiles. In *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 347–353. IEEE, 2020.
- [31] Cheng Xiang, Png Chin Yong, and Lim Swee Meng. Design of multiple-level hybrid classifier for intrusion detection system using bayesian clustering and decision trees. *Pattern Recognition Letters*, 29(7):918–924, 2008.
- [32] Kamran Shafi and Hussein A Abbass. An adaptive genetic-based signature learning system for intrusion detection. *Expert Systems with Applications*, 36(10):12036–12043, 2009.
- [33] Xiaojun Tong, Zhu Wang, and Haining Yu. A research using hybrid rbf/elman neural networks for intrusion detection system secure model. *Computer physics communications*, 180(10):1795–1801, 2009.
- [34] Weiming Hu, Wei Hu, and Steve Maybank. Adaboost-based algorithm for network intrusion detection. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 38(2):577–583, 2008.
- [35] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang. A new approach to intrusion detection using artificial neural networks and fuzzy clustering. *Expert systems with applications*, 37(9):6225–6232, 2010.
- [36] Muna Mhammad T Jawhar and Monica Mehrotra. Design network intrusion detection system using hybrid fuzzy-neural network. *International Journal of Computer Science and Security*, 4(3):285–294, 2010.

REFERENCES

- [37] Jordi Domingo-Pascual, Pietro Manzoni, Sergio Palazzo, Ana Pont, and Caterina Scoglio. *NETWORKING 2011: 10th International IFIP TC 6 Networking Conference, Valencia, Spain, May 9-13, 2011, Proceedings*. Springer Science & Business Media, 2011.
- [38] Ming-Yang Su. Real-time anomaly detection systems for denial-of-service attacks by weighted k-nearest-neighbor classifiers. *Expert Systems with Applications*, 38(4):3492–3498, 2011.
- [39] Seungmin Lee, Gisung Kim, and Sehun Kim. Self-adaptive and dynamic clustering for online anomaly detection. *Expert Systems with Applications*, 38(12):14891–14898, 2011.
- [40] Carlos A Catania, Facundo Bromberg, and Carlos García Garino. An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection. *Expert Systems with Applications*, 39(2):1822–1829, 2012.
- [41] Zubair Md Fadlullah, Hiroki Nishiyama, Nei Kato, and Mostafa M Fouda. Intrusion detection system (ids) for combating attacks against cognitive radio networks. *IEEE network*, 27(3):51–56, 2013.
- [42] Warusia Yassin, Nur Izura Udzir, Zaiton Muda, and Md Nasir Sulaiman. Anomaly-based intrusion detection through k-means clustering and naives bayes classification. 2013.
- [43] Neda Afzali Seresht and Reza Azmi. Mais-ids: A distributed intrusion detection system using multi-agent ais approach. *Engineering Applications of Artificial Intelligence*, 35:286–298, 2014.
- [44] Wei-Chao Lin, Shih-Wen Ke, and Chih-Fong Tsai. Cann: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, 78:13–21, 2015.
- [45] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis, and Robert Atkinson. Threat analysis of iot networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE, 2016.

- [46] Piyush A Sonewar and Sonali D Thosar. Detection of sql injection and xss attacks in three tier web applications. In *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, pages 1–4. IEEE, 2016.
- [47] Binhan Xu, Shuyu Chen, Hancui Zhang, and Tianshu Wu. Incremental k-nn svm method in intrusion detection. In *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pages 712–717. IEEE, 2017.
- [48] Elike Hodo, Xavier Bellekens, Ephraim Iorkyase, Andrew Hamilton, Christos Tachatzis, and Robert Atkinson. Machine learning approach for detection of nontor traffic. In *Proceedings of the 12th international conference on availability, reliability and security*, pages 1–6, 2017.
- [49] Mohamad Nazrin Napiah, Mohd Yamani Idna Bin Idris, Roziana Ramli, and Ismail Ahmedy. Compression header analyzer intrusion detection system (cha-ids) for 6lowpan communication protocol. *IEEE Access*, 6:16623–16638, 2018.
- [50] AL-Hawawreh Muna, Nour Moustafa, and Elena Sitnikova. Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information security and applications*, 41:1–11, 2018.
- [51] Sara Mohammadi, Hamid Mirvaziri, Mostafa Ghazizadeh-Ahsaei, and Hadis Karimipour. Cyber intrusion detection by combined feature selection algorithm. *Journal of information security and applications*, 44:80–88, 2019.
- [52] Fadi Salo, Ali Bou Nassif, and Aleksander Essex. Dimensionality reduction with ig-pca and ensemble classifier for network intrusion detection. *Computer networks*, 148:164–175, 2019.
- [53] Mojtaba Eskandari, Zaffar Haider Janjua, Massimo Vecchio, and Fabio Antonelli. Passban ids: An intelligent anomaly-based intrusion detection system for iot edge devices. *IEEE Internet of Things Journal*, 7(8):6882–6897, 2020.
- [54] Hery Frédéric Rakotomalala and André Totohasina. On hierarchical classification implicative and cohesive-based: Application on analysis of the computing curricula and students abilities according the anglo-saxon model. In *Fourth International Congress on Information and Communication Technology: ICICT 2019, London, Volume 1*, pages 83–90. Springer, 2019.

- [55] Md Delwar Hossain, Hideya Ochiai, Fall Doudou, and Youki Kadobayashi. Ssh and ftp brute-force attacks detection in computer networks: Lstm and machine learning approaches. In *2020 5th international conference on computer and communication systems (ICCCS)*, pages 491–497. IEEE, 2020.
- [56] MA Khan. Hcrnnids: hybrid convolutional recurrent neural network-based network intrusion detection system. *processes*. 2021; 9 (5): 834.
- [57] Amit Kumar Balyan, Sachin Ahuja, Umesh Kumar Lilhore, Sanjeev Kumar Sharma, Poongodi Manoharan, Abeer D Algarni, Hela Elmannai, and Kaamran Raahemifar. A hybrid intrusion detection model using ega-pso and improved random forest method. *Sensors*, 22(16):5986, 2022.
- [58] Yazan Otoum, Dandan Liu, and Amiya Nayak. Dl-ids: a deep learning-based intrusion detection framework for securing iot. *Transactions on Emerging Telecommunications Technologies*, 33(3):e3803, 2022.
- [59] Syed Muhammad Danish, Arfa Nasir, Hassaan Khaliq Qureshi, Ayesha Binte Ashfaq, Shahid Mumtaz, and Jonathan Rodriguez. Network intrusion detection system for jamming attack in lorawan join procedure. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.
- [60] Prasanta Gogoi, DK Bhattacharyya, Bhogeswar Borah, and Jugal K Kalita. Mlh-ids: a multi-level hybrid intrusion detection method. *The Computer Journal*, 57(4):602–623, 2014.
- [61] Christopher D McDermott and Andrei Petrovski. Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks. *International journal of computer networks and communications*, 9(4), 2017.
- [62] Wei Zong, Yang-Wai Chow, and Willy Susilo. Dimensionality reduction and visualization of network intrusion detection data. In *Information Security and Privacy: 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3–5, 2019, Proceedings 24*, pages 441–455. Springer, 2019.
- [63] Amir Andalib and Vahid Tabataba Vakili. A novel dimension reduction scheme for intrusion detection systems in iot environments. *arXiv preprint arXiv:2007.05922*, 2020.

REFERENCES

- [64] Sharfuddin Khan, E Sivaraman, and Prasad B Honnavalli. Performance evaluation of advanced machine learning algorithms for network intrusion detection system. In *Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India*, pages 51–59. Springer, 2020.
- [65] Meliboev Azizjon, Alikhanov Jumabek, and Wooseong Kim. 1d cnn based network intrusion detection with normalization on imbalanced data. In *2020 international conference on artificial intelligence in information and communication (ICAIIC)*, pages 218–224. IEEE, 2020.
- [66] Kristopher Kristopher Robert Kendall. *A database of computer attacks for the evaluation of intrusion detection systems*. PhD thesis, Massachusetts Institute of Technology, 1999.
- [67] Kamran Siddique, Zahid Akhtar, Farrukh Aslam Khan, and Yangwoo Kim. Kdd cup 99 data sets: A perspective on the role of data sets in network intrusion detection research. *Computer*, 52(2):41–51, 2019.
- [68] Donald Welch and Scott Lathrop. Wireless security threat taxonomy. In *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 2003.*, pages 76–83. IEEE, 2003.
- [69] Natarajan Meghanathan, Selma Boumerdassi, Nabendu Chaki, and Dhinaharan Nagamalai. *Recent Trends in Network Security and Applications: Third International Conference, CNSA 2010, Chennai, India, July 23-25, 2010 Proceedings*, volume 89. Springer, 2010.
- [70] Miel Verkerken, Laurens D’hooge, Tim Wauters, Bruno Volckaert, and Filip De Turck. Unsupervised machine learning techniques for network intrusion detection on modern data. In *2020 4th Cyber Security in Networking Conference (CSNet)*, pages 1–8. IEEE, 2020.
- [71] Caiming Liu and Yan Zhang. An intrusion detection model combining signature-based recognition and two-round immune-based recognition. In *2021 17th International Conference on Computational Intelligence and Security (CIS)*, pages 497–501. IEEE, 2021.

- [72] Amar Meryem and Bouabid EL Ouahidi. Hybrid intrusion detection system using machine learning. *Network Security*, 2020(5):8–19, 2020.
- [73] Mohanad Sarhan, Siamak Layeghy, Nour Moustafa, and Marius Portmann. Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management*, 31(1):3, 2023.
- [74] 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)*, pages 1–6, 2015. doi: 10.1109/MilCIS.2015.7348942.
- [75] Nour Moustafa and Jill Slay. The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set. *Information Security Journal: A Global Perspective*, 25(1-3):18–31, 2016.
- [76] Nour Moustafa, Jill Slay, and Gideon Creech. Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. *IEEE Transactions on Big Data*, 5(4):481–494, 2019. doi: 10.1109/TBDDATA.2017.2715166.
- [77] Nour Moustafa, Gideon Creech, and Jill Slay. Big data analytics for intrusion detection system: Statistical decision-making using finite dirichlet mixture models. *Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications*, pages 127–156, 2017.
- [78] Damien Desfontaines and Balázs Pejó. Sok: differential privacies. *arXiv preprint arXiv:1906.01337*, 2019.
- [79] Ying Zhao and Jinjun Chen. A survey on differential privacy for unstructured data content. *ACM Computing Surveys (CSUR)*, 54(10s):1–28, 2022.
- [80] Cynthia Dwork. Differential privacy. In *International colloquium on automata, languages, and programming*, pages 1–12. Springer, 2006.
- [81] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. Differential privacy techniques for cyber physical systems: a survey. *IEEE Communications Surveys & Tutorials*, 22(1):746–789, 2019.

REFERENCES

- [82] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017.
- [83] Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečný, Sanjiv Kumar, and H Brendan McMahan. Adaptive federated optimization. *arXiv preprint arXiv:2003.00295*, 2020.