



NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF COMPUTER INFORMATION SYSTEMS

**PERFORMANCE EVALUATION OF MACHINE LEARNING TECHNIQUES IN
CYBERSECURITY**

M.Sc. THESIS

Adam Muhammad ISA

NICOSIA

February, 2024

Adam Muhammad ISA

**Performance Evaluation of
Machine Learning
Techniques in
Cybersecurity**

Master Thesis

2024

NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF COMPUTER INFORMATION SYSTEMS

**PERFORMANCE EVALUATION OF MACHINE LEARNING
TECHNIQUES IN CYBERSECURITY**

M.Sc. THESIS

Adam Muhammad ISA

Supervisor




Assoc. Prof. Sahar EBADINEZHAD

NICOSIA

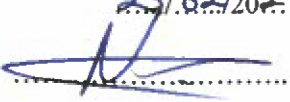
February, 2024

Approval

We certify that we have read the thesis submitted by Adam Muhammad ISA, titled “**Performance Evaluation of Machine Learning Techniques in Cybersecurity**” and that in our combined opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Educational Sciences.

Examining Committee	Name-Surname	Signature
Head of the Committee:	Prof. Dr. Nadire Cavus	
Committee Member*:	Assoc. Prof. Dr. Nuriye Sancar	
Supervisor:	Assoc. Prof. Sahar Ebadinezhad	

Approved by the Head of the Department

23/02/2024


Prof. Dr. Nadire Cavus

Head of Department

Approved by the Institute of Graduate Studies

...../20...
Prof. Dr. Kemal Hüsnü Can Başer
Head of the Institute



Declaration

I hereby declare that all information, documents, analysis, and results in this thesis have been collected and presented according to the academic rules and ethical guidelines of the Institute of Graduate Studies, Near East University. I also declare that as required by these rules and conduct, I have fully cited and referenced information and data that are not original to this study.

Adam Muhammad ISA

...../...../.....

Acknowledgments

I would like to express my heartfelt gratitude to Almighty Allah for granting me the strength and guidance to embark on this academic journey. I extend my sincere appreciation to my supervisor, Assoc. Prof. Sahar Ebadinezhad, whose guidance, expertise, and patience have been invaluable in shaping this thesis. Your mentorship has been a source of inspiration. To my father, Alh. Muhammad ISA, your unwavering support and belief in my potential have been my driving force. I am profoundly grateful for your encouragement and sacrifices. My deepest appreciation goes to my brother, Alh. Muhammad Bello, whose boundless kindness and unwavering support have played a pivotal role in helping me achieve this goal.

I am thankful to my entire family for their constant encouragement, understanding, and prayers throughout this challenging yet rewarding endeavour. Your contributions have not gone unnoticed by all those who have supported and believed in me along this academic journey. Thank you for being part of this milestone in my life.

Table of Contents

Approval.....	i
Declaration	ii
Acknowledgments.....	iii
List Table	viii
List of Figures	ix
List of Abbreviations.....	x
Abstract	xii

CHAPTER I

Introduction	1
1.1 Background	1
1.2 The Study's Unique Contribution	3
1.3 Importance of the Thesis Statement	3
1.4 Contribution of the Thesis to Computer Information Systems (CIS)	3
1.5 Problem Statement Based on the Literature	4
1.6 Proposed Research Questions	4
1.7 Limitations of the Thesis	5
1.8 Thesis Structure and Chapters Overview	6

CHAPTER II

Literature review	7
2.1 Introduction to the literature review	7
2.1.1 Overview of machine learning techniques in Cybersecurity	7
2.1.2 Usual datasets for the performance evaluation of ML in cybersecurity	8
2.1.3 Theoretical Foundations of Machine Learning in Cybersecurity	11
2.1.4 The importance of performance evaluation in machine learning in cybersecurity	11
2.2 Machine Learning Techniques	13
2.2.1 Introduction to machine learning techniques	13

2.2.1	Supervised learning techniques and their applications in cybersecurity	14
2.2.2	Unsupervised learning techniques and their applications in cybersecurity	14
2.2.3	Reinforcement learning techniques and their applications in cybersecurity	15
2.2.4	Deep learning techniques and their applications in cybersecurity	16
2.2.5	Hybrid ML techniques and their applications in cybersecurity	17
2.3	Performance Evaluation of Machine Learning Techniques in Cybersecurity	18
2.3.1	Introduction to performance evaluation in machine learning in cybersecurity	18
2.3.2	Metrics for performance evaluation in ML in cybersecurity	18
2.3.3	Evaluation methodologies for ML techniques in cybersecurity.	21
2.3.4	Challenges and limitations of performance evaluation in ML in cybersecurity	21
2.4	Applications of Machine Learning Techniques in Cybersecurity	22
2.4.1	Introduction to applications of machine learning in cybersecurity	22
2.4.2	Network security and intrusion detection using machine learning	23
2.4.3	Malware detection and classification using machine learning	24
2.4.4	Cyber-attack attribution and prediction using machine learning	24
2.4.5	Security operations centre (SOC) automation using machine learning	25
2.4.6	Cyber threat intelligence and analysis using machine learning	26
2.5	Existing Research Gaps and Future Research Directions	26
2.5.1	Identification of gaps in the existing literature on performance evaluation of machine learning techniques in cybersecurity	26
2.5.2	Potential research directions to address the identified gaps and limitations	29
2.6	Conclusion of the literature review chapter	30

CHAPTER III

Methodology	31
3.1 Research Design	31
3.1.1 Search Strategy.....	31
3.1.2 Inclusion and Exclusion Criteria.....	32
3.1.3 Selection Processes	33
3.1.4 Quality Assessment.....	34

CHAPTER IV

Result and Discussion	36
4.1 Overview of the Studies Considered	36
4.1.1 RQ1. The current literature reveals various gaps and limitations.....	36
4.1.2 RQ2. Various ML approaches are utilized in the field of cybersecurity	38
4.1.3 RQ3. ML techniques in the field of cybersecurity face several challenges	40
4.1.4 RQ4. ML techniques in the field of cybersecurity are using a variety of metrics and evaluation methodologies	43
4.1.5 RQ5. The Utilization of Supervised Learning Techniques in the Field of Cybersecurity	44
4.1.6 RQ6. Unsupervised learning techniques for cybersecurity.....	47
4.1.7 RQ7. Utilization of Deep Learning in Cybersecurity	48
4.1.8 RQ8. Utilization of Reinforcement Learning in Cybersecurity.....	50
4.1.9 RQ9. Emerging Trends and Approaches in the Evaluation of ML Techniques for Cybersecurity	53
4.2 Source of Data	55

CHAPTER V

Discussion	64
-------------------------	----

CHAPTER VI

Conclusion and Future work	68
6.1 Future Directions	70
6.2 Recommendation	72
Reference.....	74
Appendix A: Ethical Committee Approval Letter	83
Appendix B: Turnitin Similarity Report	84

List Table

Table 1.1	5
Table 2.1	10
Table 3.1	31
Table 3.2	32
Table 3.3	35
Table 4.1	56

List of Figures

Figure 3-1	33
-------------------------	-----------

List of Abbreviations

SLR:	Systematic Literature Review
AI:	Artificial Intelligence
ML:	Machine Learning
DL:	Deep Learning
CIS:	Computer Information Systems
IDS:	Intrusion Detection Systems
ICT:	Information and Communication Technology
NIDS:	Network Intrusion Detection Systems
DoS:	Denial of Service
DDoS:	Distributed Denial of Service
RL:	Reinforcement Learning
ACC:	Accuracy
Pre:	Precision
Rec:	Recall
F1:	F1-score
TPR:	True Positive Rate
FPR:	False Positive Rate
ROC:	Receiver Operating Characteristic
AUC:	A Higher Area Under the Curve
MCC:	Matthew Correlation Coefficient
IF:	Isolation Forest
SVM:	Support Vector Machines
OCSVM:	One Class Support Vector Machine
SOC:	Security Operations Centre

MITM:	Man-in-the-Middle
CNN:	Convolutional Neural Network
RNN:	Recurrent Neural Network
KNN:	K-Nearest Neighbors
NN:	Neural Network
GAN:	Generative Adversarial Network
DBNs:	Deep Belief Networks
DT:	Decision Trees
NB:	Naive Bayes
DGA:	Domain Generation Algorithm
Cont.:	Continue
DGA:	Domain Generation Algorithm
MLP:	Multilayer Perceptron
FL:	Federated Learning
DLHA:	Double-Layered Hybrid Approach
DnRaNN:	Dense Random Neural Network
FPGA:	Field Programmable Gate Array

Abstract

Performance Evaluation of Machine Learning Techniques in Cybersecurity

ISA Adam Muhammad

Supervisor: Assos. Prof. Dr. Sahar Ebadinezhad

Department of Computer Information Systems

February, 2024, 104 Pages

As the digital environment undergoes continuous development, the risks that are a threat to our digital ecosystems also increase. The application of machine learning (ML) methods in the field of cybersecurity has become a valuable asset in safeguarding against a continuously growing range of cyber-attacks. This thesis presents a systematic literature review (SLR) that aims to comprehensively examine the complexity of evaluating machine learning (ML) approaches in the field of cybersecurity. Through this review, the paper reveals valuable insights as well as the obstacles associated with this evaluation process.

The systematic literature review examines nine primary research questions, providing perspectives on the utilization of outdated datasets, the necessity of automation in addressing rising risks, the search for effective cyber threat detection, the significance of real-time factors, and the integration of real-time data analytics. This study investigates the utilization of ensemble learning techniques and the integration of explainable artificial intelligence (AI) approaches as a means of enhancing cybersecurity. This paper discusses the efficacy of deep learning architectures and the dual nature of machine learning, wherein its uses can have positive as well as negative consequences. The importance of employing up-to-date evaluation techniques is emphasized, along with the significance of integrating models through ensemble learning.

We place a strong emphasis on how critical it is to automate security systems so they can quickly adapt to new threats and modernize datasets to reflect current threat environments. Moreover, the study presents a comprehensive analysis of the evaluation of machine learning techniques in the field of cybersecurity, highlighting specific areas that require improvement, opportunities for innovation, and other possibilities for further research. As the progression of the digital domain persists, our ability to counteract cyber dangers must progress in parallel, driven by the knowledge gained via this investigation.

Keywords: *Machine learning, cybersecurity, performance evaluation, deep learning, artificial intelligence*

Özet

Siber Güvenlikte Makine Öğrenimi Tekniklerinin Performans Değerlendirmesi

ISA Adam Muhammad

Danışman: Doc. Prof. Dr. Sahar Ebadinezhad

Bilgisayar Bilişim Sistemleri Bölümü

Şubat, 2024, 104 Sayfa

Dijital ortam sürekli geliştikçe dijital ekosistemlerimizi tehdit eden riskler de artıyor. Siber güvenlik alanında makine öğrenimi yöntemlerinin uygulanması, sürekli büyüyen siber saldırılara karşı korunmada değerli bir varlık haline geldi. Bu tez, siber güvenlik alanında makine öğrenimi yaklaşımlarını değerlendirmenin karmaşıklığını kapsamlı bir şekilde incelemeyi amaçlayan sistematik bir literatür taraması sunmaktadır. Bu inceleme sayesinde makale, değerli görüşlerin yanı sıra bu değerlendirme süreciyle ilgili engelleri de ortaya koymaktadır.

Sistematik literatür taraması, güncel olmayan veri kümelerinin kullanımı, artan risklere yönelik otomasyonun gerekliliği, etkili siber tehdit algılama arayışı, gerçek zamanlı faktörlerin önemi ve gerçek-zamanlı faktörlerin entegrasyonu hakkında perspektifler sağlayan dokuz temel araştırma sorusunu inceliyor. zaman veri analitiği. Bu çalışma, siber güvenliği artırmanın bir yolu olarak toplu öğrenme tekniklerinin kullanımını ve açıklanabilir yapay zeka (AI) yaklaşımlarının entegrasyonunu araştırıyor. Bu makale, derin öğrenme mimarilerinin etkinliğini ve makine öğreniminin ikili doğasını tartışmaktadır; burada kullanımları hem olumlu hem de olumsuz sonuçlara yol açabilmektedir. Modellerin toplu öğrenme yoluyla entegre edilmesinin önemi ile birlikte güncel değerlendirme tekniklerini kullanmanın önemi vurgulanmaktadır.

Yeni tehditlere hızlı bir şekilde uyum sağlayabilmeleri ve veri kümelerini mevcut tehdit ortamlarını yansıtacak şekilde modernize edebilmeleri için güvenlik sistemlerini otomatikleştirmenin ne kadar kritik olduğuna güçlü bir vurgu yapıyoruz. Ayrıca çalışma, siber güvenlik alanında makine öğrenimi tekniklerinin değerlendirilmesine ilişkin kapsamlı bir analiz sunarak iyileştirme gerektiren belirli alanları, yenilik fırsatlarını ve daha ileri araştırmalar için diğer olasılıkları vurguluyor. Dijital alanın ilerlemesi devam ettikçe, bu araştırmayla elde edilen bilgiler doğrultusunda siber tehlikelere karşı koyma becerimizin de paralel olarak ilerlemesi gerekiyor.

Anahtar Kelimeler: Makine öğrenimi, siber güvenlik, performans değerlendirme, derin öğrenme, yapay zeka

CHAPTER I

Introduction

This section of the thesis provides context for the study, outlines the research problem, explains why it was conducted, and lays out its goals, objectives, and research questions. The importance of the thesis, its delimitation, the scope of the research, and the way it was carried out were all further discussed.

1.1 Background

Artificial intelligence (AI), with a particular focus on Machine Learning (ML) and Deep Learning (DL), has recently seen substantial utilization within the context of cybersecurity. The increase in AI adoption can be attributed to the exponential growth of Internet-connected devices and the continuous advancements in AI technologies in recent years. These AI-driven approaches have greatly influenced various facets of cybersecurity, ranging from intrusion detection to virus detection and spam filtering. Their application has produced promising results, often outperforming traditional cybersecurity strategies that rely on signatures and predefined rules. Despite the clear benefits of AI-based approaches, an ongoing challenge remains. Many ML and DL models are implemented as "black-box" systems, rendering them opaque and inscrutable. As a result of this opaqueness, both security professionals and regular users are often in the dark as to why these AI systems make the decisions that they do. In cybersecurity circumstances, confidence, transparency, and accountability are largely dependent on knowing the reasoning behind a choice. (Zhang et al., 2022). Addressing this issue is critical, since AI continues to play an increasingly important role in protecting digital ecosystems.

The field of cybersecurity is characterized by its ever-changing nature, as it involves the implementation of many strategies and practices to protect computer systems from harmful attacks or to proactively prevent such threats. The scenario might be likened to a complex competition with two central actors: one being the competitor who constantly searches for and exploits weaknesses in computer systems with the aim of obtaining illegal entry points, stealing valuable information, or carrying out other malicious activities. On the contrary, the defence must actively improve the system and strongly combat these attacks. The covert nature of cyberattacks

necessitates perpetual readiness, as attackers rarely send notifications before initiating the attack, (Bland et al., 2020). Cybersecurity is experiencing constant change due to the rapid progress of technology and the growing complexity of cyber threats. The implementation of ML methods has become an important driving force in various fields where the analysis and processing of large datasets are crucial. Machine learning algorithms enable the identification of complex patterns, behaviors, and anomalies within these datasets. The techniques primarily belong to two essential categories, namely prediction and classification. In the context of classification tasks, machine learning models are trained using a set of representative data samples to find patterns and make predictions that are useful for putting new things into categories that have already been set (Prazeres et al., 2023). The integration of machine learning has significantly transformed organizations' approaches to cybersecurity. The integration of machine learning into cybersecurity improves its capacity for protection through the use of intelligent algorithms, proactive measures, cost-effective solutions, and improved effectiveness. As a result, machine learning approaches are increasingly important in various applications within the field of cybersecurity. However, despite the ongoing achievements, numerous obstacles remain, requiring collective endeavours to guarantee the dependability of machine learning systems. In the area of cyberspace, there exist individuals with evil intentions who are actively trying to attack vulnerabilities in machine learning techniques. The presence of these enemies poses major challenges to the reliability of machine learning technologies. However, machine learning-based cybersecurity systems demonstrate the ability to detect and interpret complex patterns, which can be utilized to prevent future intrusions and adjust to changing conditions. Furthermore, they enable cybersecurity teams to adopt a proactive approach to mitigating threats and effectively responding to active attacks, intrusions, or instances of data breaches. In addition, by automating routine tasks, ML-based solutions enable individuals and organizations to optimize resource utilization (Sarker, 2022). In this ever-evolving landscape, it is imperative to address the constantly changing tactics of adversaries. It involves a continuous evaluation of the efficacy of machine learning techniques in the domain of cybersecurity, the identification of any potential weaknesses or limitations, and the invention of new strategies for improvement.

1.2 The Study's Unique Contribution

This research adds to the growing body of literature on cybersecurity by bringing together the outcomes of a systematic literature review. It compiles a wide range of studies to shed light on the complexities, opportunities, and future prospects of using machine learning in the field of cybersecurity. It also points out where more research is needed by pointing out gaps and limitations in the current literature. Study findings also stress the need for accessibility, efficiency, and practicality in ML-driven cybersecurity systems. It also highlights the importance of regularly updating datasets and evaluation criteria to keep up with the ever-evolving nature of cyber threats.

1.3 Importance of the Thesis Statement

In the fields of ML and cybersecurity, this thesis is of the greatest relevance. Its thorough assessment of the present state of machine learning applications in cybersecurity makes it an invaluable resource for academics, industry professionals, and authorities. This study's findings can direct future research efforts, allowing them to better address the gaps and issues uncovered. In addition, by highlighting best practices and encouraging the development of more robust and transparent systems, the thesis helps the growth of ML-driven cybersecurity. It acknowledges the importance of machine learning in protecting against new forms of cybercrime and stresses the importance of constant research and development in this field.

1.4 Contribution of the Thesis to Computer Information Systems (CIS)

This thesis provides a significant contribution to the discipline of Computer Information Systems (CIS) through the consolidation and analysis of the current body of knowledge regarding machine learning in the context of cybersecurity. It provides a starting point for additional study into ML-driven security solutions. The thesis highlights the usefulness of real-time data analytics, ensemble learning, and explainable AI in boosting cybersecurity measures, and stresses the importance of aligning ML approaches with the growing threat scenario. This thesis intends to further the application of machine learning in CIS by addressing the limitations identified in the literature, ultimately leading to the development of more effective and efficient cybersecurity systems.

1.5 Problem Statement Based on the Literature

The existing body of research on this aspect of the utilization of machine learning in cybersecurity draws attention to a number of challenges as well as knowledge gaps. Outdated data sets, the requirement for new automation to deal with growing threats, the significance of effective and quick threat detection, and the incorporation of real-time data analytics into performance evaluation systems are all challenges that need to be overcome. In addition to that, there is a significant demand for ensemble learning approaches, explainable artificial intelligence, and deep learning architectures. The body of research also places an emphasis on the dual nature of machine learning applications, which can either be utilized to improve cybersecurity or can be used by attackers to their benefit. The researchers emphasize, as a last point but certainly not the least of them, the significance of integrating ensemble learning approaches into model construction and making use of relevant evaluation criteria.

1.6 Proposed Research Questions

The main objective of this systematic literature review is to conduct a thorough analysis of the evaluation of machine learning techniques in the context of cybersecurity. This review aims to address significant questions in research by conducting a thorough analysis and synthesis of the existing literature. The focus is on understanding the complexities of machine learning's adoption in the field of cybersecurity. **Table 1.1** provides an overview of the research questions.

Table 1.1

Provides a clear overview of the research questions and their corresponding variables.

R/Q	Variables
What are the current gaps and limits in the available literature in terms of evaluating the performance of ML approaches in cybersecurity?	Gaps in existing literature regarding performance evaluation of ML techniques in cybersecurity. Limitations in existing literature regarding performance evaluation of ML techniques in cybersecurity
What are the many forms of ML approaches that are utilized in the field of cybersecurity?	Types of ML techniques used in cybersecurity. Applications of ML techniques in cybersecurity
What are the specific challenges and limitations encountered in ML techniques in the cybersecurity domain?	The challenges that have arisen when applying ML techniques to cybersecurity. Specific limitations that relate to the application of ML methods in the field of cybersecurity
What are the commonly used metrics and evaluation methodologies for assessing the performance of ML techniques in cybersecurity?	Commonly used metrics for assessing the performance of ML techniques in cybersecurity. Evaluation methodologies employed for assessing the performance of ML techniques in cybersecurity
What are the cybersecurity applications of supervised learning techniques, as well as their drawbacks and vulnerabilities?	Applications of supervised learning techniques in cybersecurity. Limitations and vulnerabilities associated with supervised learning techniques in cybersecurity
How are unsupervised learning techniques used in cybersecurity for evaluating performance, and what conclusions may be drawn from unlabelled data?	Cybersecurity applications of unsupervised learning techniques. Cybersecurity insights from unlabelled data using unsupervised learning techniques
How are DL techniques utilized in cybersecurity, and what are their benefits and limitations relative to conventional ML techniques?	Exploring the utilization of DL techniques in cybersecurity, investigating the advantages and limitations of these techniques in comparison to traditional ML methods.
What are the uses for reinforcement learning in cybersecurity, and how can those applications help improve security measures?	Applications of reinforcement learning in the field of cybersecurity. Enhancing cyberspace security with reinforcement learning techniques
What new patterns and orientations are developing in the performance evaluation of ML techniques in cybersecurity?	New developments in the performance evaluation of ML methods for cybersecurity. Future directions in the performance evaluation of ML techniques in cybersecurity

1.7 Limitations of the Thesis

Like every systematic literature review, this thesis has limitations that require careful examination. The scope of this review was deliberately confined to articles published within the preceding five years, which, while ensuring the inclusion of contemporary research, may have excluded useful information from older studies. Moreover, the selection process was rigorous, with papers included solely if they aligned with the specified inclusion criteria, potentially excluding relevant research that did not precisely fit them. Furthermore, it is worth noting that the evaluation focused solely on utilizing full-text open-source papers, which may have resulted in the exclusion of beneficial information that was found in subscription-based or restricted-access journals. Ultimately, the research was carried out over four various

databases, potentially excluding a comprehensive range of existing literature within the discipline. Future research in this field should aim to address these limitations by including a wider variety of articles, covering a wide range of databases, languages, and publication formats. This would enable a more thorough and inclusive review of the topic at hand.

1.8 Thesis Structure and Chapters Overview

The structure of the chapters in this thesis has been carefully designed to facilitate a thorough investigation of the chosen topic area. In Chapter 2, a thorough literature review will be presented, offering insights into the existing body of the subject matter. Chapter 3 will provide insight into the methodology utilized for conducting the systematic literature review, shedding light on the research process. In the subsequent section, Chapter 4 will present the research findings, providing significant insights and observations. Chapter 5 will contain a comprehensive discussion, summarizing the significant discoveries and outlining possible directions for future research. At the end of Chapter 6 will serve as the concluding section of this thesis, summarizing the main results and offering recommendations based on the research outcomes.

CHAPTER II

Literature review

This section of the thesis provides a comprehensive review and concise summary of relevant literature that relates to the utilization of machine learning techniques in the domain of cybersecurity.

2.1 Introduction to the literature review

With the increasing use of machine learning techniques in cybersecurity to prevent and detect cyber threats, many studies have been conducted to evaluate their performance. These studies involve analysing different machine learning models to identify their strengths and weaknesses and improve their effectiveness in detecting and responding to cyber-attacks. Researchers have conducted literature reviews to provide an overview of the current state of research on this topic. These reviews summarize relevant studies, highlight the gaps and limitations in existing research, and provide insights for future research in this field.

2.1.1 Overview of machine learning techniques in Cybersecurity

Machine learning techniques have emerged as valuable tools in the field of cybersecurity. With the increasing complexity and sophistication of cyber threats, traditional rule-based systems alone are often insufficient to detect and respond to attacks effectively. Machine learning offers a data-driven approach to cybersecurity by leveraging algorithms that can learn patterns, detect anomalies, and make predictions based on large volumes of data. In the realm of cybersecurity, machine learning finds application in various areas. One such area is intrusion detection, where ML models analyse network traffic, user behavior, and system logs to identify abnormal activities indicating potential attacks. By continuously learning from historical data, these models can adapt to new attack vectors, enhancing the accuracy of intrusion detection systems. Another critical use case is malware detection, where machine learning algorithms scrutinize file characteristics and behavior to differentiate between benign software and malicious programs. By training on extensive datasets of known malware samples, ML models can identify new and previously unknown malware variants, including zero-day attacks, (Wazid et al., 2022).

Machine learning techniques also play a pivotal role in risk assessment and vulnerability management. By analysing system configurations, patch levels, and other

relevant data, ML models can pinpoint potential vulnerabilities and prioritize remediation efforts. This proactive approach aids organizations in addressing security weaknesses before they can be exploited. Furthermore, machine learning contributes to threat intelligence and information sharing. By analysing vast amounts of data from diverse sources, ML algorithms can uncover emerging threats, uncover hidden relationships between cyber incidents, and provide actionable insights to security teams. However, it is important to recognize that machine learning is not a cure-all for all cybersecurity challenges. ML models can be susceptible to adversarial attacks, where attackers manipulate input data to deceive models and bypass security measures. Ensuring the robustness and resilience of ML models against such attacks remains an ongoing area of research and development. As noted by, Mijwil et al. (2023), the increasing prevalence and interconnectedness of electronic devices have led to a greater risk of cyber threats, such as data theft. As a result, researchers have proposed using machine learning techniques to address these threats, although the field is still in its early stages. The use of ML is considered to be a promising approach to addressing the constantly evolving and diverse nature of cyber threats in the technology industry. However, despite the promise of ML in cybersecurity, it is difficult to rely on any one solution because the threat landscape is continuously changing. Yet, security experts may better defend against new attacks and safeguard electronic devices and networks by utilizing ML techniques like anomaly detection, predictive modelling, and threat intelligence analysis. Moreover, ML may play a variety of other functions in cybersecurity beyond vulnerability detection. Cybersecurity threats are being fought off with the help of ML methods, such as systems that detect intrusions. Cybersecurity uses ML; a variety of techniques and strategies have been created to identify dangers in the cyber-sphere. Even though viruses, whose processes can be blocked by them, typically evolve and improve more quickly than malware detection tools, software applications (virus protection) can be used to identify viruses with favourable performance. However, the threats' quick growth prompted the introduction of learning approaches for the recognition of unidentified ransomware attacks, including a range of ML algorithms (Martínez Torres et al., 2019).

2.1.2 Usual datasets for the performance evaluation of ML in cybersecurity

This subsection will provide a commonly used of the various dataset that are employed by machine learning techniques within the context of cybersecurity. Data science plays a vital role in bolstering cybersecurity efforts. Through the application

of sophisticated machine and deep learning algorithms, it becomes feasible to analyse large volumes of data and uncover meaningful patterns that can help detect and mitigate potential cyberattacks. By utilizing these techniques, organizations can proactively identify weaknesses in their systems, take preventive measures, and respond effectively to cybersecurity incidents. Ultimately, the objective is to fortify information technology infrastructure and ensure the integrity, confidentiality, and availability of data and systems. **Table 2.1** presents a compilation of significant datasets utilized in cybersecurity research. These datasets serve as valuable resources for evaluating various aspects of cybersecurity, including intrusion detection, anomaly detection, attack detection, and network penetration. However, the most commonly used cybersecurity datasets, suffer from a serious problem in that many of them are not updated in specific directions. For example, the most well-known datasets for spam detection date back over a decade ago. Privacy and ethical concerns could be to blame for this phenomenon, (Zhang et al., 2022). As a result, the most recent types of cyberattacks were not included in the public datasets on cyberattacks, which made it difficult to train ML applications to create defences against cyberattacks. Even while the industrial datasets for industries like healthcare, innovative farming, and smart mobility contain more recent samples than the datasets for cyber assaults, these datasets should also be updated because cyber-attacks are currently getting more sophisticated and diversified.

Table 2.1
The most notable datasets employed in cybersecurity research

UNSW-NB15	NSL-KDD	MAWI	KDD'99 Cup	KYOTO	ISCX'12	DARPA	CTU-13	CICIDS2017	CAIDA	Bot-IoT	Dataset
Sarker (2022)	Ahsan et al. (2022)	Ferrag et al. (2020)	Ferrag et al. (2023)	Alshammari. (2020)	Sarker, (2022)	Shaukat et al. (2020)	Berghout et al. (2022)	Ahisan et al. (2022)	Ferrag et al. (2020)		Reference
UNSW-NB15 was created using the IXIA Perfect Storm tool in the Cyber Range Lab of UNSW Canberra, The UNSW-NB15 dataset incorporates contemporary synthetic attack activities and behaviors. It includes 49 features and covers nine attack types. With 100 GB of captured traffic, this dataset allows for the evaluation of classification models and the analysis of various attack scenarios.	This dataset is a revised version of the KDD'99 Cup dataset, addressing issues present in the original dataset. It eliminates redundant records and resolves biases towards frequent records, making it a more balanced and improved resource for machine learning-based attack detection models.	The MAWI dataset aids researchers in detecting anomalies by providing data retrieved from Japanese network research institutions. It includes labeled traffic deviations and is regularly updated to include traffic from various applications and malware.	Widely used for evaluating anomaly detection, the KDD'99 Cup dataset consists of 41 features. It has been employed since 1999 to identify anomalies in computer systems and categories into probing, remote-to-local (R2L), user-to-remote (U2R), and denial-of-service (DoS) categories.	Alshammari. (2020)	ISCX'12, produced by the Canadian Institute for Cybersecurity, the ISCX'12 dataset focuses on machine learning-based attack detection and network penetration. It contains 19 features, with significant portion of the traffic (19.11%) attributed to distributed denial-of-service attacks. (DDoS) attacks.	This dataset comprises intrusion detection data, including LLDOS-1.0 and LLDOS2.0.2. It contains information on connections between source and destination IP addresses, categorized by the MIT Lincoln Laboratory. The dataset is instrumental in evaluating attacks and detecting intrusions.	This extensive dataset captures botnet traffic from a Czech university in 2011. It aims to provide real-world botnet traffic scenarios mixed with regular and background traffic. The dataset encompasses 13 different botnet samples, making it useful for botnet-related research.	Data from Monday, July 3, 2017, to Friday, July 7, 2017, are included in this dataset. The CICIDS2017 traces, including data from a DDoS attack in 2007. It incorporates threats including Brute Force SSH, DoS, Heartbleed, Web Attack, infiltrating Botnet and DDoS, DoS, OS, activity on the Internet and Brute force denial of service attacks. based on the employed protocols.	The CAIDA dataset includes distributed denial of service (DDoS) attack traffic and regular traffic traces, including data from a DDoS attack in 2007. It enables the evaluation of machine learning-based models for identifying DDoS activity on the Internet and studying the impact of denial of service attacks. based on the employed protocols.	Bot-IoT simulates the Internet of Things (IoT) environment and features reliable traffic. It is designed in the Cyber Range Lab of UNSW Canberra, offering files in different formats such as PCAP and CSV. The dataset covers DDoS, DoS, OS, service scan, keylogging, and data exfiltration attacks, categorized based on the employed protocols.	Overview

In summary, machine learning techniques offer invaluable capabilities in the field of cybersecurity. From intrusion detection to malware detection, risk assessment to threat intelligence, ML empowers organizations to bolster their defenses, proactively respond to evolving threats, and safeguard their systems and data.

2.1.3 Theoretical Foundations of Machine Learning in Cybersecurity

The study of techniques, theories, and useful applications is the main objective of the field of artificial intelligence (AI), which belongs to computer science. Artificial Neural Networks (ANNs), a subfield of artificial intelligence, were first developed as a result of efforts to design streamlined models that were inspired by the way neurons function in biological systems like the human brain. ML is a branch of AI in which algorithms are trained on data to create models that can make decisions or predictions without explicit programming. Moreover, a variety of fields have used machine learning in a wide range of strategies. In the area of cybersecurity, ML approaches are being utilized to improve safety measures and detect various types of automated attacks and emerging risks, including the detestation of phishing websites. To evaluate trends and learn from data, these apps make use of ML algorithms, which enable the creation of proactive and successful protection systems in the world of technology, (Shaukat et al., 2020).

Machine learning is a crucial tool for tackling cybersecurity issues since it allows automated analysis of massive amounts of data to quickly identify and counter threats. The theoretical foundations and fundamental ideas must be understood, though, to effectively utilize machine learning's potential in cybersecurity. Moreover, cybersecurity is a widely recognized domain where ML models find significant use within Internet of Things (IoT) contexts. ML, which encompasses deep learning, has demonstrated its efficacy in safeguarding cyber environments from cyber threats. One of the hazards that exist within this context are insider threats, (Aloraini et al., 2022).

2.1.4 The importance of performance evaluation in machine learning in cybersecurity

Machine learning and cybersecurity are mutually beneficial and play a vital role in enhancing each other's effectiveness. The integration of these fields offers several advantages. One advantage is the improved security of ML models. As mentioned, ML models are vulnerable to various attacks that can negatively affect their functionality, performance, and predictive capabilities. However, by implementing

specific cybersecurity measures, these detrimental incidents can be mitigated. The application of cybersecurity protocols safeguards the functioning, performance, and input datasets of ML models, ensuring the generation of accurate predictions and reliable outcomes, (Wazid et al., 2022). Thus, the importance of performance evaluation in machine learning (ML) in cybersecurity lies in its ability to drive advancements in this field and involve various stakeholders. By evaluating the performance of ML in cybersecurity, we can achieve the following benefits:

Enhanced performance of ML techniques cybersecurity domain: Evaluating ML algorithms within cybersecurity systems, such as intrusion detection systems, leads to improved performance. This includes higher accuracy, detection rates, and lower false positive rates. ML techniques like supervised learning, unsupervised learning, reinforcement learning, and deep learning algorithms can be tailored to the specific communication environment and associated systems. Performance evaluation provides clear guidance for stakeholders to enhance future ML applications in cybersecurity.

Efficient detection: ML models integrated into cybersecurity methods have demonstrated effectiveness in detecting zero-day attacks, which are unknown and novel malware attacks. These ML models leverage the collection and matching of specific features to identify malicious programs. Through automated detection, ML models can accurately identify zero-day attacks. Conducting performance evaluations in cybersecurity and machine learning helps identify the strengths and weaknesses of detection techniques and provides direction for improvement, leading to more effective and refined detection of zero-day attacks.

Our research, emphasizes the significance of performance evaluation in machine learning for cybersecurity. Evaluating the performance of ML algorithms in cybersecurity systems, such as intrusion detection, enhances their overall performance and contributes to the advancement of the field. Additionally, performance evaluation plays a critical role in effectively detecting zero-day attacks, providing valuable insights into the strengths and weaknesses of detection techniques. This evaluation process guides stakeholders in improving the performance and capabilities of ML in cybersecurity.

2.2 Machine Learning Techniques

In this section, we explore the various machine-learning techniques that have been applied in the area of cybersecurity. Machine learning, a branch of AI, provides a wide variety of techniques for addressing cybersecurity issues. These techniques enable systems to learn from data, adapt to new threats, and improve security measures. From supervised and unsupervised learning to deep learning and reinforcement learning, we explore the basic methodologies that strengthen cybersecurity experts to detect, prevent, and respond to cyber threats effectively. Each technique has its unique strengths and applications, contributing to the comprehensive landscape of cybersecurity defense.

2.2.1 Introduction to machine learning techniques

A machine learning technique can be defined as "the process of generating ML models by utilizing ML algorithms upon certain training data" as a result. To create systems that can make decisions on their own, ML seeks to automate decision-making. A training stage is used to facilitate learning. An ML model is produced by teaching a computer to study some training data using a particular ML technique. Such a model, which incorporates all the information learned during the training stage, includes a function to create decisions according to subsequent data. Before implementing a machine learning model in the real world, its performance must be assessed. To do this, a limited collection of the test dataset is reviewed by a machine learning model, and the forecasts it produces are then either checked by users or compared to a specified objective reality, (Apruzzese et al., 2023). ML techniques are a collection of mathematical methods used to address high non-linear issues in various fields, including predictions, segmentation, data linkage, and data modelling. The development of security risk systems has utilized ML techniques, such as Bayesian systematized neural networks, Naive Bayes, Bayesian classifiers, support vector machines (SVM), neural network classification techniques, or self-organization visualizations, (Ortiz and Reinerman-Jones, 2015). Machine learning is a method of artificial intelligence (AI) that could quickly glean useful information from big datasets. Three types of ML strategies have been identified: reinforcement learning technique, unsupervised learning technique, and supervised learning technique, (Basheer and Ranjana, 2022).

2.2.1 Supervised learning techniques and their applications in cybersecurity

Supervised learning is a type of machine learning where the algorithm is provided with various instances and their corresponding solutions, which are used to build the model. Some of the commonly used supervised techniques include artificial neural networks such as the multilayer perceptron, decision trees, and support vector machines, as noted by Torres et al. (2019). However, as stated by Apruzzese et al. (2020) supervised classifiers are vulnerable to adversarial evasion, and there are several limitations in current solutions. Many solutions suffer from degraded performance without adversarial perturbations, are unable to handle new attack variants, and are limited to specific machine learning algorithms.

2.2.2 Unsupervised learning techniques and their applications in cybersecurity

Unsupervised learning technique: These methods are typically utilized in what is known as exploratory data analysis. They are frequently employed when the classes are already known and we need to confirm the training procedure and the variable set selection. "The clustering algorithm (k-means algorithm) and Kohonen's self-organizing maps are the two most well-known algorithms of unsupervised learning. Different goals for this kind of learning could include categorization, the creation of hierarchies, the reduction of dimensions, or interpretation and visualization" (Torres et al., 2019). Moreover, one fundamental difference between supervised learning and unsupervised learning is in the presence or absence of class labels. Unsupervised learning involves working with unlabeled input samples, where the assessment of the trained model is not entirely dependent on accurately mapping input to output classes. Instead, it focuses on accomplishing an additional objective (Liang et al., 2019). However, in cybersecurity, unsupervised learning techniques are used to gain insights from unlabelled data, spot patterns or structures, or extrapolate important information. Malware acts in a dynamic and evasive way, frequently concealing its presence to elude detection and protection methods, making it difficult to identify and mitigate, (Mijwil et al.,2023). As a result, unsupervised learning techniques like clustering, anomaly detection, and association rule mining are increasingly being applied to identify unknown threats and lower the risk of cyberattacks. These techniques can aid security analysts in identifying possible threats and taking prompt corrective action.

2.2.3 Reinforcement learning techniques and their applications in cybersecurity

Reinforcement learning occupies an intermediate position between supervised and unsupervised learning paradigms. Unlike supervised learning, reinforcement learning does not rely on labelled input data. Instead, it operates based on reward signals associated with the input, aiming to enhance the decision-making capabilities of the overarching model. Usually, to achieve this, one must maximize the cumulative benefits of iterative execution. The representation of this concept can be illustrated through the perception-action-learning loop. There are two primary techniques employed in reinforcement learning, namely policy search and value function approximation. The first one, which is policy search, refers to the process of seeking an optimal policy through the utilization of either gradient-based or gradient-free methodologies. An instance of this is “Google's Alpha Go,” which uses policy search as its foundation. It possesses the ability to acquire knowledge and improve its performance without any involvement or interaction from humans, ultimately attaining a state of superiority. And secondly, the value function approximation is a technique that aims to estimate the anticipated rewards associated with different activities, with the ultimate goal of achieving an improved learning process and outcomes. The primary constituent of the value function is the state-action value function, sometimes referred to as the quality function (Liang et al., 2019). In addition, an agent learns to make decisions by interacting with the environment using the ML technique known as reinforcement learning (Apruzzese et al., 2023). Reinforcement learning is also known as learning with a critic because the algorithms receive information to correct any incorrect predictions. The algorithm has not, however, been instructed on how to make corrections. Instead, until it discovers the right response, the algorithm must determine and test several options, (Shaukat et al., 2020). Moreover, numerous industries, including robotics, gaming, and autonomous systems, have successfully used reinforcement learning. In different contexts and for different purposes, adversarial machine learning is frequently linked with reinforcement learning due to their shared focus on interactions between different agents. This shared focus also means that both techniques can be targeted by adversarial attacks. However, adversarial machine learning can also be used to plan attacks, as well as to develop defenses against these threats through techniques like adversarial training. Overall, the relationship between adversarial machine learning and reinforcement learning is complex and multifaceted,

with both offensive and defensive applications in various domains, including cybersecurity, (Apruzzese et al., 2020).

2.2.4 Deep learning techniques and their applications in cybersecurity

Machine learning's deep learning (DL) branch, which can handle complex data types like images or unstructured text and take into account temporal connections, has several advantages. One of its advantages is that it can be applied to reinforcement learning as well as supervised and unsupervised learning, (Apruzzese et al., 2023). This means that it can find patterns and relationships in data without knowing what to look for, or it can learn from labelled data to recognize patterns and make predictions. For data analysis and decision-making in a variety of domains, including cybersecurity, deep learning can offer effective tools. Moreover, Torres et al., (2019) stated that a recent area of study in ML is the “deep learning technique”; The creation of a neural network that imitates the human intellect for analytical learning is the driving force behind it. It imitates how the human brain interprets data like sights, sounds, and messages. At the moment, models based on machine learning and deep learning are being used practically everywhere within the realm of cybersecurity to detect and respond to intrusions, (Shaukat et al., 2020). The major difference between deep learning and classical machine learning lies in their performance with varying amounts of security data. Deep learning algorithms demonstrate superior performance when dealing with large volumes of data, which allows them to uncover intricate patterns and relationships in complex cybersecurity datasets. On the other hand, classical machine learning algorithms tend to excel when working with smaller datasets, where they can efficiently generalize patterns and make accurate predictions. Therefore, deep learning is particularly advantageous in scenarios where the availability of data is abundant, enabling it to leverage the power of neural networks to process and understand vast amounts of information. Conversely, in situations when data is limited or scarce traditional machine learning approaches can nevertheless offer reliable and effective solutions by effectively extracting crucial information from smaller datasets. The best technique for a given cybersecurity task or challenge must be chosen by taking into account the positive and negative aspects of each approach. Exploring ways to combine the advantages of deep learning and traditional machine learning techniques could open the way for more powerful and comprehensive security solutions as the field of cybersecurity continues to develop, (Sarker et al., 2020).

However, DL still has several limitations but can manage data without requiring human intervention. DL methods demand a vast quantity of data and expensive hardware to perform better than ML methods.

2.2.5 Hybrid machine learning techniques and their applications in cybersecurity

Hybrid machine learning approaches have become prominent in the realm of cybersecurity, offering a comprehensive strategy for addressing the always-changing variety of cyber threats. Integrating abuse and anomaly detection technologies in cybersecurity systems synergistically enhances their performance and efficacy. Misuse detection, which is distinguished by the utilization of rule-based systems and signature-based approaches, demonstrates effectiveness in the identification of established attack patterns. However, it has difficulties when confronted with emerging or complex threats. In contrast, anomaly detection demonstrates a notable proficiency in the identification of unknown threats by detecting deviations from established patterns of typical behavior. By integrating these two approaches, hybrid systems can leverage the collective intelligence of both methodologies. Because of the inclusion of a misuse detection component, these systems are capable of effectively identifying known attacks. Additionally, their anomaly detection capabilities enable them to remain attentive against a variety of new threats, (Vinayakumar et al., 2019; Xin et al., 2018). An area where hybrid machine learning techniques have gained significant prominence is in the field of intrusion detection systems (IDS). These systems function as the digital protectors of computer networks, continuously surveilling for indications of unlawful entry, malicious acts, or unusual behavior. The integration of misuse and anomaly detection techniques in hybrid IDS can provide a more comprehensive and robust defense mechanism. The ability to promptly recognize established attack patterns, such as those linked to malware or prevalent exploits, while also adjusting to newly developed threats that display unusual behaviors, is a quality they possess, (Kim and Pak, 2021).

Moreover, the utilization of hybrid machine learning techniques plays a crucial role in effectively tackling a recurring obstacle in the domain of cybersecurity, namely the issue of false positives. By corroborating findings from misuse and anomaly detection, these systems can reduce the probability of raising alarms for benign activities that may appear suspicious but are not indicative of a cyberattack. Consequently, this process improves the efficacy of cybersecurity teams by enabling

them to concentrate on authentic threats rather than being burdened with the task of sorting through a large volume of erroneous warnings.

2.3 Performance Evaluation of ML Techniques in Cybersecurity

The spotlight in this part is on machine learning's performance evaluation in cybersecurity. metrics for ML in cybersecurity performance evaluation, methodologies for measuring the performance of ML algorithms in cybersecurity, as well as the difficulties and limitations of such performance measurement.

2.3.1 Introduction to performance evaluation in machine learning in cybersecurity

In multiple cybersecurity applications, machine learning techniques play an essential part in the early identification and prediction of various threats. These applications include spam classification, fraud detection, malware detection, phishing, dark web or deep-web sites, and intrusion detection. The shortage of accessible staff members knowledgeable in specialized cybercrime detection technologies can be alleviated with machine learning techniques. In addition, robust methods are required to detect and respond appropriately to cyberattacks of the latest generation, which are automated and evolutionary. Machine learning is one of the possible ways to act rapidly against such assaults since ML can learn from experiences and adapt to newer attacks on time. This makes ML one of the possible solutions to act swiftly against such attacks (Shaukat et al., 2020).

Furthermore, ML is being utilized more and more in cybersecurity to identify and stop security risks. The efficiency of machine learning models, however, depends on how successfully they can identify these threats. An essential phase in the machine learning process is performance evaluation, which involves comparing a model's performance to a set of measures. This makes it easier to evaluate how effectively the model works at spotting and avoiding security issues as well as to pinpoint areas that could want improvement, (Apruzzese et al., 2023).

2.3.2 Metrics for performance evaluation in machine learning in cybersecurity

Machine learning (ML) based systems, especially for tasks involving threat detection in cybersecurity, benefit greatly from evaluation to determine their efficacy. The effectiveness of a given ML method in detecting threats can be evaluated using

performance metrics. Choosing the right metrics is crucial, as using the wrong ones might inject bias into the evaluation process and have an effect on the approach's dependability and generalizability, as noted by Juba and Le, (2019). The attack detection domain makes use of performance indicators as objective benchmarks to evaluate the ML models. These metrics are derived from four fundamental statistics: True Positive (TP), which represents instances of attacks that were correctly detected; True Negative (TN), which represents instances of attacks that were correctly detected; False Positive (FP), which defines instances of attacks that were incorrectly detected; and False Negative (FN), which defines instances of attacks that were incorrectly detected. The performance metrics that are frequently employed include:

- Accuracy (Acc): This commonly used metric evaluates the overall correctness of the ML strategy by estimating the percentage of correctly identified assaults and benign occurrences. However, it may not be appropriate for unbalanced datasets because it does not account for the percentage of false positives, which could lead to erroneous conclusions.
- Precision (Pre): measures the percentage of instances of attacks that were accurately identified out of all cases that were classified as attacks. When the precision value is low, there is a greater likelihood that neutral occurrences will be incorrectly labelled as malicious ones.
- Recall (Rec): Also referred to as sensitivity, recall quantifies the percentage of accurately recognized attack instances among all actual assault cases in the dataset. A poor recall rating indicates many false negatives due to missed detections.
- The F1-score (F1): is a measure of accuracy that takes into account both precision and recall. It is highly suggested for analysing unbalanced data sets.
- The ROC curve is a measure that evaluates the costs and benefits of different TP and FP rates. A decent ROC curve, determined by comparing the true positive rate (TPR) to the false positive rate (FPR), will be more than 50%.
- The AUC is a metric for measuring the area under the receiver operating characteristic (ROC) curve, which shows how well an indicator can distinguish between attack and normal cases. A higher area under the curve (AUC) indicates a more accurate classification.
- Testing Time: This term describes how long it takes for a ML model or method to detect anything.

- Training Time: This metric represents how long it takes a machine learning model or methodology to develop a model for detecting patterns.
- The Matthew Correlation Coefficient (MCC) is a comprehensive measure of correlation that takes into account all four primary statistics. When the MCC value is positive, the prediction is accurate; when it is zero, the prediction is random; and when it is negative, the prognosis is unfavourable.
- Cohen's Kappa: Kappa evaluates the consistency between the positive (attack) label and the detection outcomes. Kappa is useful for evaluating the quality of the ML model, especially in highly imbalanced data circumstances, where a value of 1 indicates perfect agreement and a score of -1 indicates perfect disagreement., (Koay et al., 2023).

The nature of the cybersecurity work and the intended outcomes of the ML-based strategy inform the selection of the most appropriate metric(s). For instance, when the classes are equal in size, accuracy, which evaluates the total correctness of predictions, is frequently utilized. However, in unbalanced datasets, when the number of attack instances is significantly less than normal instances, accuracy may not be sufficient. Precision, recall, F1 score, and AUC-PR are more illuminating in this situation because they place more emphasis on accurately identifying the minority class (i.e., attacks) and so reduce the effect of imbalanced data. Moreover, the metrics selected ought to be in keeping with the practical implications of the cybersecurity application. For instance, limiting false negatives (missed detections) is prioritized in some security-critical cases, even if this results in an increase in false positives (false alarms). However, in cases where resources are scarce, it may be more important to focus on reducing false positives to avoid wasting both resources, (Shaukat et al., 2020).

In addition, the presence of adversarial attacks must be taken into account while evaluating ML models for cybersecurity. Adversarial attacks are when data is manipulated on purpose to deceive a machine learning model. As a result, the model's robustness against hostile scenarios may not be completely captured by conventional measurements. The model's resilience to such attacks is measured with specialized measures like robustness evaluation and adversarial accuracy, (Xin et al., 2018).

In conclusion, the accuracy of the results and the generalizability of the method depend critically on the performance measures used to evaluate ML-based approaches

to attack detection. An objective and complete evaluation, leading to better cybersecurity solutions, requires judicious and context-aware metric selection.

2.3.3 Evaluation methodologies for machine learning techniques in cybersecurity

Methodologies for evaluating the performance of ML techniques in cybersecurity are crucial. The success of the ML model is measured by setting evaluation measures, choosing acceptable datasets, and applying suitable validation techniques. Cross-validation (Apruzzese et al. 2023; Xin et al. 2018), Holdout validation (Tanner et al., 2019), Receiver Operating Characteristic (ROC) curve, and Confusion matrix (Al-Taleb & Saqib, 2022; Martínez T. et al., 2019; Rashid et al., 2020) are a few typical evaluation methodologies for ML algorithms in cybersecurity. In general, the choice of the right approach for evaluating an ML model depends on the particular problem being studied and the datasets that are available for analysis. It's crucial to carefully choose appropriate evaluation metrics and validation methods to accurately assess the performance of the ML model. So, the appropriate evaluation methodology should be chosen based on the problem at hand and the data available, and it's important to select suitable evaluation metrics and validation methods to ensure an accurate assessment of the ML model's performance.

2.3.4 Challenges and limitations of performance evaluation in machine learning in cybersecurity

In, Shaukat et al. (2020), examined the "current Difficulties of Employing ML methods in cybersecurity" and explained the significant existing challenges and limitations encountered during the implementation of ML techniques in cybersecurity. Moreover, every ML approach has advantages and disadvantages. There isn't a method for machine learning that can be called the best without any restrictions. The fact that gathering data is a time-consuming and arduous process is one of the major challenges ML approaches confront. Most publicly accessible datasets contain redundant or missing values and are out of date. Furthermore, the statement suggests that there is a significant gap between research and practice in the adoption of machine learning techniques in cybersecurity. This is evident from the fact that the use of machine learning in cybersecurity is still in its early stages, as pointed out by Apruzzese et al. (2023). Despite the potential benefits of machine learning in cybersecurity, such as enhancing threat detection, response, and mitigation, there are

still significant challenges and barriers to its adoption in practice. This gap between research and practice highlights the need for further research to address the challenges and limitations of machine learning in cybersecurity and bridge the gap between theoretical knowledge and practical application.

2.4 Applications of Machine Learning Techniques in Cybersecurity

In this section, we look into the practical applications of machine learning techniques in the context of cybersecurity. Machine learning has transformed how entities protect their digital assets and networks. By utilizing the power of data-driven techniques, cybersecurity experts are able to detect threats, analyse vulnerabilities, and strengthen defenses. From intrusion detection and threat intelligence to anomaly detection and malware analysis, we investigate the wide variety of applications where machine learning plays a pivotal role in improving cybersecurity measures. These applications become the frontline safeguarding against developing cyber threats in an increasingly digital world.

2.4.1 Introduction to applications of machine learning in cybersecurity

Machine learning has emerged as a strong force in the domain of cybersecurity, resulting in the development of new techniques to bolster our digital defenses against the continuous destruction of online cyberattacks. Its influence is far-reaching and can be seen in many different aspects of information security, such as vulnerability assessment and intrusion detection. In recent years, the integration of ML has transformed the way we see risks in the digital landscape and how we defend ourselves against them. ML techniques are being utilized in various areas such as Intrusion Detection (Basheer & Ranjana, 2022), Malware classification (Apruzzese et al., 2023), and Network Traffic Analysis: In their study, Agnew et al. (2022) elaborate on the contributions that ML has made to network traffic analysis. In this day and age of ever-increasing data flows, machine learning algorithms sift through enormous amounts of data to find patterns that could be missed by more traditional computer systems. This analytical acuity not only improves network efficiency but also reveals risks that have been hiding in the shadows. Finally, vulnerability assessment: According to Shaukat et al. (2020) vulnerability assessment is one of the many applications that benefits greatly from the capabilities of machine learning. ML-driven assessments perform extensive scans of systems to look for vulnerabilities and locate points of entry that

could be exploited by attackers. This proactive strategy enhances preventative procedures, making it possible for organizations to address vulnerabilities before they are exploited. Note, the speed and accuracy of an organization's threat detection and response processes can be significantly improved when they make use of machine learning's capability. Their cybersecurity posture becomes characterized by their adaptability in the face of constantly changing threats. Innovation grows and digital ecosystems are strengthened as a result of the mutually beneficial link between machine learning and cybersecurity.

The future holds the potential for even larger synergy between machine learning and cybersecurity, as models are expected to grow more sophisticated, flexible, and capable of fending off attacks that are increasingly complicated. With machine learning as a reliable ally, organizations are able to negotiate the digital frontier with fortitude and self-assurance, and they are better prepared to face new challenges head-on. In an ever-evolving digital landscape, the combination of machine learning and cybersecurity is a light of hope that will ensure the safety of both systems and data. As technology continues to progress, so too do the risks that threaten them.

2.4.2 Network security and intrusion detection using machine learning

Intrusion Detection: Basheer and Ranjana (2022) shed light on the ways in which ML approaches have reimagined the process of intrusion detection. Organizations can significantly improve their ability to detect and prevent efforts to gain unauthorized access by training models to recognize aberrant behaviour amidst the background noise of digital data. Intrusion detection systems that are powered by ML offer a shield in real time against the dangers posed by cyberattacks and vigilantly monitor the boundaries of digital spaces. One of the most important aspects of cybersecurity, which also encompasses network security and intrusion detection, is identifying and stopping illegal access to computer networks. Because it enables automated analysis of massive volumes of network data to find unusual patterns and potential threats, ML is a viable method for improving network security and intrusion detection. To aid in the real-time detection and prevention of attacks, ML methods can be used to build prediction models that can recognize well-known attack signatures and aberrant network activities. Support vector machines, decision trees, and neural networks are a few of the frequently used ML techniques for network security and

intrusion detection. Furthermore, ML-based network security and intrusion detection has been the subject of numerous studies and research papers. “hybrid machine learning model for network intrusion detection”, for instance, is proposed in a recent publication by Talukder et al. (2023) that improves detection rates while guaranteeing dependability by combining DL and ML. another paper by Bari et al. (2023), also explored intrusion detection based on vehicle controller area network.

2.4.3 Malware detection and classification using machine learning

The classification of Malware The research carried out by Apruzzese et al. (2023) highlights the key role that ML plays in the classification of malware. Despite the rise in the quantity and sophistication of malicious software, ML models are able to differentiate between benign and malicious code with ease. In order to protect one's systems and data against sneaky cyber infections, it is essential to have the ability to quickly classify the many kinds of threats. However, malware is frequently used by attackers in the fourth stage of a cyberattack to keep access to the compromised system. Trojans, backdoors, and rootkits are examples of malware that can be used to connect an attacker to a compromised machine. ML algorithms can be used to detect this infection. These algorithms can examine the packets of network data and spot odd patterns that might point to the existence of malware. Support vector machines (SVM) is one such method that has demonstrated success in identifying malware traffic packets (Ahsan et al., 2022). SVM is a kind of ML algorithm that may gain knowledge from labeled data and apply it to categorize incoming data points as either normal or abnormal. Cybersecurity experts can detect and respond to intrusions more quickly by using SVM for malware detection.

2.4.4 Cyber-attack attribution and prediction using machine learning

The process of identifying the source of a cyber-attack, known as cyber-attack attribution, can be challenging due to the evasive strategies employed by attackers. As a promising approach for both attribution and prediction of cyberattacks, ML looks at attack patterns and features to identify the most likely source and anticipate upcoming attacks. ML algorithms can be used to analyse a variety of data, such as the type of malware used, the patterns of network traffic, and the language or location of the attacker, to ascribe a cyberattack. Finding the attack's likely source can be helped by this analysis. As an alternative, machine learning can be used to examine massive

amounts of data to spot trends and abnormalities that might point to an impending attack, (Bitirgen and Filik, 2023).

Additionally, ML models are extensively used for analyzing and predicting various phenomena. However, these models can be vulnerable to different types of attacks that can adversely impact their performance. Some common attacks include dataset poisoning attacks, model poisoning attacks, privacy breach attacks, membership inference attacks, and runtime disruption attacks. These attacks have the potential to manipulate the ML models, leading to incorrect predictions and compromised results. Nonetheless, in a dataset poisoning attack, an attacker intentionally inserts adversarial examples or manipulated data into the training dataset, causing the ML model to generate inaccurate predictions. On the other hand, in a model poisoning attack, the focus of the attacker is to corrupt the models by tampering with their internal workings and modifying the model parameters. Moreover, Privacy breach attacks involve exposing sensitive data and attempting to retrieve valuable information from the ML model. Membership inference attacks are a specific type of privacy breach attack where an attacker tries to infer whether a specific data point was part of the training dataset used for the ML model. Furthermore, runtime disruption attacks aim to disrupt the workflow of the ML model during its execution, leading to inaccurate prediction results. These attacks target the execution process and can significantly affect the model's performance. Therefore, to mitigate these security risks, it is essential to employ various cybersecurity mechanisms such as encryption techniques, signature generation and verification techniques, and hashing mechanisms. These mechanisms help protect the ML models and associated datasets from attacks, ensuring the integrity and confidentiality of the data. By implementing robust cybersecurity measures, we can enhance the security of ML models, obtain reliable outcomes, and improve the accuracy of predictions, (Wazid et al., 2022).

2.4.5 Security operations centre (SOC) automation using machine learning

The automated analysis of massive amounts of security-related data to find patterns and anomalies has made ML look like a potential technique for SOC automation. Building predictive models that can quickly identify and address security issues is possible with the use of ML techniques. To examine network traffic logs and spot patterns of behavior that can point to a security breach, for instance, ML can be

utilized, (Agyepong et al., 2023). Therefore, organizations may increase the effectiveness and efficiency of their security operations, lower the risk of security breaches, and strengthen their overall security posture by automating security processes using ML. However, when using ML for SOC automation, it is important to carefully take into account things like the accuracy of the models, the quality of the data, and the possibility of false positives and false negatives.

2.4.6 Cyber threat intelligence and analysis using machine learning

Machine learning-based cyber threat intelligence and analysis involves the use of cutting-edge algorithms and techniques to gather and analyse massive amounts of data from multiple sources to identify potential cyber risks and take preventative action. This strategy makes use of ML to automatically analyse data and find trends that could point to an impending assault, (Kattamuri et al., 2023). Therefore, machine learning-based cyber threat intelligence and analysis are crucial elements in modern cybersecurity, assisting firms in staying ahead of changing threats and defending sensitive data from online attacks.

2.5 Existing Research Gaps and Future Research Directions

The present state of research at the intersection of machine learning and cybersecurity is reviewed in this section. The use of machine learning techniques has tremendous potential, however, it also raises a number of challenges and research gaps that have not yet been well addressed. We look at existing knowledge gaps and the expanding areas that need more investigation. We hope that by highlighting these gaps, future research efforts can be launched to strengthen the interplay between machine learning and cyber security. This section highlights the importance of continuous innovation and research in order to navigate the dynamic and complex cybersecurity landscape efficiently.

2.5.1 Identification of gaps in the existing literature on performance evaluation of machine learning techniques in cybersecurity

Mijwil et al. (2023) researched the role of machine learning and deep learning techniques in cybersecurity, focusing on their ability to reduce intrusions and attacks on computers and their applications in various cyber contexts. They also suggested that future studies should explore the implementation of these techniques in predicting

and classifying cybersecurity data to assess their effectiveness and achieve optimal execution. However, the limitations of this work are not explicitly stated, and further research may be needed to evaluate the validity and generalizability of their findings. Additionally, it is important to note that the effectiveness of machine learning and deep learning techniques in cybersecurity may depend on the specific context and may not always be applicable or effective in all situations.

Mazhar et al. (2023) conducted a study on Cyber Security Attacks and Solutions for Smart Grid. The paper lacks a performance evaluation and a clear comprehensive approach for addressing the persistent issues and challenges associated with cybersecurity in smart grids. It emphasizes the need for novel approaches that can resolve these issues without compromising the network's efficiency and usefulness but does not offer specific recommendations or solutions for addressing these challenges. As a result, future research is needed to address these limitations and develop practical and effective approaches to enhancing cybersecurity in smart grid infrastructures.

Al-Taleb and Saqib, (2022) introduced a new hybrid deep learning model that utilizes a CNN and a QRNN to improve feature extraction, and classification accuracy, and decrease FPR in threat categorization. However, in terms of limitations, the claim that the model can accurately analyse and classify data in real time for CTI in smart cities is untested.

Berghout et al. (2022), provided a direction for solutions and discussed various drawbacks and challenges of using ML for cybersecurity in their review paper. However, it's important to note that their study was limited to the area of smart grids, which restricts its generalizability to other ML for cybersecurity domains.

Rashid et al. (2020), evaluated the effectiveness of various machine learning techniques and ensemble techniques in detecting IoT cyber threats in smart cities. However, the evaluation was limited to only two datasets, which may not provide a comprehensive understanding of their effectiveness. The authors suggested that future research could involve evaluating the performance of these techniques on a wider range of datasets to gain a better understanding of their potential impact. The results of their evaluation indicated that the ensemble techniques, particularly stacking classifiers, can better detect cyberattacks in smart city systems, which could have economic and social implications that warrant further investigation.

In Martínez T. et al. (2019), conducted a limited review of “machine learning techniques applicable to cybersecurity”, which did not include a performance evaluation. To provide a more comprehensive analysis of the effectiveness of these techniques, future work could involve a broader scope that encompasses a more comprehensive range of machine learning techniques and evaluates their performance in detecting various cybersecurity threats. Additionally, exploring potential applications of machine learning techniques in improving network and system security could be beneficial.

The limitation of the study by Xin et al. (2018) is that despite the value placed on “machine learning and deep learning techniques” for network analysis and intrusion detection, the best technique for intrusion detection has not yet been identified. The authors concluded that each approach has its pros and cons, and choosing one technique over another is challenging. In future work, researchers could explore further to identify the most effective technique for intrusion detection by conducting comparative studies of various approaches. They could also investigate how to combine different techniques to improve the accuracy of intrusion detection systems. Moreover, it would be beneficial to develop new approaches that address the limitations of current techniques, such as the vulnerability of machine learning models to adversarial attacks.

The limitation of the study presented by Shaukat et al. (2020) is that the comparative analysis of ML techniques applied to detect cybersecurity threats was limited to only six ML models and three threats to cyberspace. As a result, the review may not provide a comprehensive evaluation of the effectiveness of machine learning models in detecting different types of cybersecurity threats. Therefore, future work in this area could explore a wider range of machine learning and deep learning techniques to detect various cybersecurity threats. This could involve expanding the scope of the study to cover more threats to cyberspace and evaluating the performance of different machine learning models on these threats. Additionally, researchers could investigate the application of machine learning models in other areas of cybersecurity, such as intrusion detection, network traffic analysis, and malware detection, to gain a more comprehensive understanding of their potential impact in the field.

2.5.2 Potential research directions to address the identified gaps and limitations

The statement suggests that to facilitate the comparison of machine learning models using different measurements, it is crucial to establish standard metrics that can be used as a benchmark. These metrics would enable researchers to evaluate and compare the performance of different models objectively. Moreover, establishing such metrics would serve as a milestone for future research by providing a basis for developing improved models, (Shaukat, L., et al., 2020). The use of standardized metrics would enhance the reproducibility of research, promote transparency in the evaluation of machine learning models, and facilitate the advancement of the field. Therefore, the establishment of standard metrics is essential to enhance the performance and effectiveness of machine learning models in cybersecurity. Moreover, reinforcement learning is a machine learning technique that enables agents to learn how to make decisions by interacting with the environment (Apruzzese et al., 2023). However, despite its effectiveness in decision-making, our review found that many researchers have not extensively discussed reinforcement learning in their work. This gap in the literature suggests a need for further research on reinforcement learning in cybersecurity and its potential applications in enhancing threat detection and response. The integration of reinforcement learning in machine learning can significantly improve the decision-making abilities of agents and enhance the performance of cybersecurity systems. Therefore, further research should focus on exploring the potential of reinforcement learning in cybersecurity and its applications in improving the effectiveness of threat detection and response systems.

Furthermore, based on the identified gaps and limitations in the existing literature on evaluating the performance of machine learning techniques in cybersecurity, several potential research directions can be explored. These include investigating the performance of a broader range of machine learning techniques, evaluating their effectiveness on diverse datasets containing various cyber threats, conducting a comparative analysis of different techniques to identify the most effective ones, exploring the potential of combining multiple techniques, investigating the interpretability and explainability of machine learning techniques, evaluating their effectiveness in real-world scenarios, and investigating the impact of various factors on their performance. Addressing these research directions can improve the

effectiveness and practicality of machine learning techniques in addressing cybersecurity challenges.

2.6 Conclusion of the literature review chapter

In conclusion, the literature analysis on the performance evaluations of machine learning techniques in cybersecurity has revealed that there is an increasing interest in using machine learning models to detect and prevent online attacks. Yet, there are still flaws and limitations in the current research, such as a lack of agreed-upon evaluation measures, a constrained comparison analysis's scope, and a practice's early phases of adoption. Future research should be directed at breaching these gaps and overcoming these constraints by investigating the use of more sophisticated machine learning techniques, testing models against a larger variety of cybersecurity threats, and creating uniform evaluation metrics. By doing this, we can boost the performance of machine learning models used for cybersecurity and better safeguard our digital assets.

CHAPTER III

Methodology

This chapter kicks off with a detailed explanation of the methodology behind the SLR. We go over the selection criteria for the studies that were included, the databases that were searched, and the keywords that were used to find the relevant literature. Screening, inclusion, and exclusion criteria are outlined comprehensively to promote transparency in the search for and selection of primary research.

3.1 Research Design

To address the study's research questions, we chose to perform a systematic literature review of existing research in the field of Machine Learning Techniques in Cybersecurity. A systematic literature review or SLR is a kind of secondary research that makes use of a predetermined procedure to seek, assess, and analyse all data pertinent to an investigation. This decision was made by following the standard procedure that is followed in the area of information systems and software engineering to ensure replicability and reduce the possibility of bias on the part of the researchers.

3.1.1 Search Strategy

Specific protocols were adhered to for this systematic literature review to ensure its quality. We searched for peer-reviewed journal articles from the last five years up to 2023. We used a broad set of keywords such as "machine learning," "artificial intelligence," "cybersecurity" "cyber security," "network intrusions" OR "intrusion detection" to guide the search. We excluded articles that were not in English, not open access, published before the last five years, and not research articles. To gather a comprehensive set of articles, we searched through multiple databases, namely IEEE, EBCO, Springer, and Science Direct, **Table 3.1** provided herein, presents a short overview of the search query keywords employed in the search strategy.

Table 3.1

Keywords search query.

Search Strategy	Keywords	Synonyms
Main	machine learning	artificial intelligence
AND	Cybersecurity	cyber security
AND	network intrusions	intrusion detection

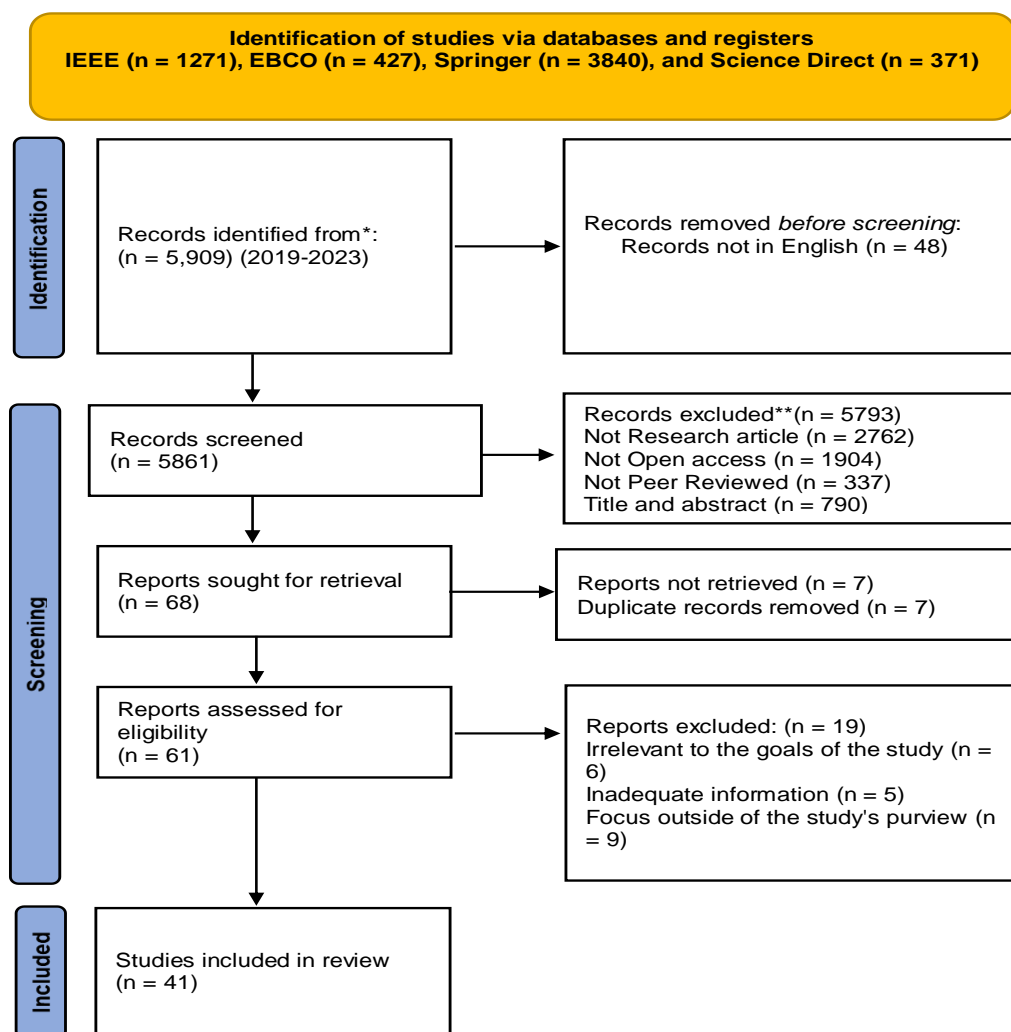
3.1.2 *Inclusion and Exclusion Criteria*

While the whole selection process undoubtedly varies based on the databases under consideration, all the selection criteria included in this study were incorporated appropriately. It is important to establish specific guidelines for including and excluding research during the selection process because this will impact the overall quality of the literature review. Please refer to **Table 3.2** for a summary of the criteria that were utilized to determine which studies should be included and which should not be included based on the results of the search process. These criteria were used to effectively complete the selection process.

Table 3.2
Inclusion and Exclusion Criteria

Criteria for Inclusion	Criteria for Exclusion:
Articles available within the four selected databases.	' Duplicate articles found between the selected databases.
Articles published in English.	' Articles published in languages other than English.
Articles with full-text accessibility online (Open access).	' Articles with full text not accessible (Not open access).
Peer-reviewed journal articles.	' Non-peer-reviewed journal articles.
Articles published in the last five years.	' Articles published before the last five years.
Research articles.	' Non-research articles.

Figure 3.1
The PRISMA flow diagram of the study



3.1.3 Selection Processes

Throughout the entire selection process, the researchers adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) guidelines, which guided the inclusion and exclusion criteria and ensured a rigorous selection process. These criteria were essential in distilling the extensive results obtained from multiple databases, namely IEEE, EBSCO, Science Direct, and Springer, to identify high-quality research journal articles. After conducting the search within the past five years and considering only papers published in English, a total of 5,909 articles were retrieved from the four databases. The initial search yielded the following numbers in each database: IEEE (n = 1271), Science Direct (n = 371), Springer (n = 3840), and EBSCO (n = 427).

Subsequently, the researchers applied additional screening criteria, excluding articles that were not peer-reviewed journal articles, not open access, or not research articles. They also assessed the titles and abstracts of the remaining articles. After this screening process, 61 articles remained for full-text assessment. The researchers thoroughly assessed these articles and, based on their quality and relevance, included 41 articles in this systematic literature review.

3.1.4 Quality Assessment

To ensure the inclusion of high-quality papers, the researchers implemented a meticulous quality assessment process. They meticulously followed the planned review methods, aligning each criterion and procedure with the study's goals and objectives. Automated tools such as Zotero were employed to facilitate the removal of duplicates, assist in the full-text assessment, manage citations, and track the overall quality of the included articles. These measures were taken to maintain the integrity and accuracy of the systematic literature review process. Furthermore, to ensure consistency throughout the investigation, we used the checklist of data extraction components presented in **Table 3.3** after reading, summarizing, paraphrasing, and synthesizing the data found in all of the primary sources, set up an detailing every data collected that can be seen in **Table 4.1** along with other data collected for further evaluation in the completion of this research.

Table 3.3*Data Extraction*

Data Items	Description
Author(s) (year)	Reference of the included study
Region/Country	Location of the study's publication
Study objectives	The primary purpose of the research
Identification of Gaps and Limitations	ML Performance Evaluation in Cybersecurity Research Gaps
Types and Applications	ML methods in cybersecurity/ML technologies in cybersecurity
Challenges and Limitations	The problems with applying ML approaches to cybersecurity and limits
Metrics methodologies	Common metrics and methodologies for the performance evaluation of ML in cybersecurity
Drawbacks and vulnerabilities	Cybersecurity supervised learning applications, limitations, and vulnerabilities
Applications of unsupervised	Cybersecurity uses unsupervised learning, unlabeled data insights
Benefits and limitations	Examining the pros and cons of deep learning in cybersecurity compared to regular machine learning.
Improving security	Cybersecurity reinforcement learning applications Strengthening cybersecurity via reinforcement learning
Future directions	New advancements and future directions ML in cybersecurity performance evaluation
Key findings	Important results from the included study

CHAPTER IV

Result and Discussion

In this section, we present the outcomes of the study, providing an extensive evaluation and interpretation of the findings. This critical section is the heart of our study, where we indicate the impact of our work and its significance. The answers to our research questions and our objectives are made clear by the facts, information, and insightful observations that we present. We go into the implications and contributions of the findings through an in-depth discussion of the research. This section acts as a bridge between our methodology and the conclusions we draw, providing a clear narrative of our research journey and its real-world significance.

4.1 Overview of the Studies Considered

An initial search of IEEE, EBSCO, Science Direct, and Springer databases yielded a total of 61 publications of interest. Using the criteria for inclusion and exclusion laid out in Chapter 3.2, a total of 41 articles were chosen for in-depth evaluation.

2.6.1 RQ1. The current literature reveals various gaps and limitations

Based on the findings, there is a clear need for standardized evaluation procedures that can be used to compare different machine learning techniques' effectiveness in the field of cybersecurity. While different research revealed different evaluation measures, there was no agreement on a standard set of indicators applicable across all fields of cybersecurity. This gap reduces the comparability of results across various research endeavors and hinders the development of best practices.

The research findings indicates that the utilization of obsolete datasets for network security research is a significant challenge, as emphasized by (De Carvalho Bertoli et al., 2021) and Vinayakumar et al. (2019), and other researchers in the field. Despite the existence of updated datasets, certain widely recognized ones, such as DARPA 1998, KDD-CUP 1999, and NSL-KDD, have been in circulation for nearly twenty years. These datasets highlight inquiries about the effectiveness of their application in addressing ongoing cyber threats. While certain datasets, such as N-BaIoT and MedBIoT, focus on specific assaults related with IoT device botnets, they may not cover the whole range of cyber risks in IoT contexts. Attacks such as

Distributed Denial of Service (DDoS) and Man-in-the-Middle (MITM) are conspicuously lacking. Nevertheless, evaluation datasets hold a pivotal role in the validation process. As highlighted by KhraISAt et al. (2019), existing datasets have been extensively used, along with their respective features and constraints. Nevertheless, a critical point of concern raised by the researchers is the outdated nature of these datasets, as they lack records of recent malware attacks. As a result, Campos et al. (2022) underline the need to include a broader range of attack types in IoT cybersecurity datasets to allow thorough evaluations of machine learning models. Moreover, Shaukat et al. (2020) discuss the urgent need for innovative automated security solutions in order to mitigate the constantly changing environment of security threats effectively. The effectiveness of automated machine learning, specifically in detecting unfamiliar cyber threats, is now undergoing research. In their study, Seo et al. (2021) highlight the significance of employing efficient and automated approaches in detecting cyber threats. The successful application of cybersecurity is depending on the capacity to quickly identify and discern threats, particularly in situations that occur in real time. Notwithstanding, the importance of timely recognition of attacks in performance evaluation is underscored by Kim and Pak, (2021). For the system to achieve effective real-time detection, it is imperative that the speed of detection exceeds that of present techniques. According to Leevy et al. (2021), the concept of system load is identified as a crucial element. Machine learning models need to have sufficient performance to operate without necessitating an excessive quantity of hardware resources. In their study, Latif et al. (2022) suggest the integration of real-time and streaming data analytics as a means for improving the performance evaluation process. This will facilitate the evaluation of the constantly changing cybersecurity landscape and ensure the relevance of assessment approaches. However, ensemble learning techniques: In their study, Yong and Gao, (2023) discuss the potential of ensemble learning techniques to enhance the overall performance of a cybersecurity system. The evaluation of measures that consider the balance between false positive rates and detection accuracy, while also accounting for the impact of false alarms in real-world scenarios, is of utmost importance. In addition, the utilization of explainable AI techniques in the field of cybersecurity is emphasized by Koay et al. (2023). Further, enhancing the clarity and accessibility of machine learning-based security systems would result in an improvement in the interpretability of their decision-making mechanisms. In addition, the study explores deep learning

architectures by Hnamte et al. (2023), Kandhro et al. (2023), Koay et al. (2023), Liang et al. (2019), and Vinayakumar et al. (2019) the study that demonstrates the usefulness of deep learning architectures, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), in improving the detection of cybersecurity vulnerabilities, and also manufacturing technologies, such as self-driving automobiles and intelligent mobile applications. These architectural designs have the potential to enhance the efficiency and accuracy of threat detection. Nevertheless, the positive and negative applications: Ferreira et al. (2023) elucidates the contradiction that comes with the utilization of machine learning in the realm of cybersecurity. Although ML has the potential to improve the decision-making capabilities and overall functionality of a system, it is important to acknowledge that attackers can exploit ML techniques to set up sophisticated attacks. The aforementioned duality highlights the significance of providing adequate consideration to both research and execution. Researchers such as Bertoli et al. (2021) and Seo et al. (2021) suggest that in order to obtain a comprehensive understanding of model performance in the field of cybersecurity, it is advisable to employ evaluation criteria beyond accuracy when testing machine learning models. To achieve viability in the actual world, these should include scalability, time and processing costs, and reliability. The utilization of ensemble learning methods for integrating several models is emphasized by Leevy et al. (2021), as they underline the potential for improving the efficacy and reliability of cybersecurity systems.

Note: to ensure the efficacy and adaptability of ML techniques against developing cyber threats, it is necessary to overcome these gaps and limits as ML in cybersecurity advances.

2.6.2 RQ2. Various ML approaches are utilized in the field of cybersecurity

Based on the research findings, cybersecurity practitioners use a variety of machine learning techniques to improve threat detection, classification, and prediction (Kandhro et al., 2023). These methods take different facets of cybersecurity concerns into account:

The utilization of machine learning techniques in intrusion detection systems (IDS) has garnered considerable attention in recent years, (Campos et al., 2022). According to Pu et al. (2021) many academic studies have been done to find ways to make cyber intrusion detection more effective using machine learning techniques, with

the main goal of increasing the rate of detection while reducing the number of false positives. Nevertheless, Shaukat et al. (2020), the SVM has gained widespread acceptance as a popular approach for the creation of IDS. The system demonstrates effective performance in detecting typical patterns within network traffic. Moreover, Siddiqi and Pak (2022) shed light on the Network Intrusion Detection System (NIDS). It is widely acknowledged that ML and DL techniques have proven to be highly effective in enhancing the capabilities of NIDS to detect and mitigate advanced network threats. Nevertheless, Kosmanos et al. (2020) and Seo et al. (2021) highlight the significance of employing Random Forest and k-NN algorithms in the context of network intrusion detection. The K-NN and Random Forest algorithms hold significant importance in the realm of network attack classification. Nonetheless, hybrid techniques refer to the integration of many methodologies or approaches to achieve a desired outcome. In their recent study, WISAnwanichthan and Thammawichai, (2021), suggest the integration of diverse learning techniques as a means to enhance attack detection capabilities. Moreover, to enhance precision, this approach leverages the benefits offered by multiple algorithms. However, Bagaa et al. (2020) comprehensively discuss several deep learning architectures, including J48, Bayes Net, RandomForest, Hoeffding, SVM, and deep learning algorithms. CNNs and RNNs, which fall under the umbrella of deep learning techniques, demonstrate notable proficiency in analyzing complex structures within cybersecurity datasets. Furthermore, ensemble learning, as discussed by Chakir et al. (2023), and Yong and Gao, (2023), is an approach utilized to train classifiers to differentiate between normal and abnormal behaviors. This approach facilitates the detection of unfamiliar threats and zero-day attacks. Additionally, according to KhraISAt et al. (2019) in the realm of machine learning, it is widely acknowledged that two principal categories of methodologies prevail: supervised and unsupervised approaches. However, Sarker, (2022) has investigated the use of various learning paradigms, including supervised, unsupervised, semi-supervised learning, and reinforcement learning. Labelled data is utilized within the context of supervised learning to detect and recognize underlying patterns. However, unsupervised learning algorithms can generate clusters or identify correlations from data that lacks explicit labels noted by Liang et al. (2019). Moreover, reinforcement learning is a strategy that entails an agent producing its training data through interactions with the environment, as defined by Sarker et al. (2020). Further, it is appropriate for training sophisticated cybersecurity systems. According to Ezugwu

et al. (2023), clustering algorithms have gained significant acceptance as an approach to detecting vulnerabilities within computer networks. Nonetheless, it aids in the detection of patterns that point to the presence of malware. Ahmad et al. (2021) and Aloraini et al. (2022), employ a variety of techniques, including supervised, semi-supervised, and unsupervised techniques, to detect traditional and adversarial behaviors. This improves the identification of abnormal behavior. However, understanding that adversaries may use machine learning for more strategic attack planning, research by Bland et al. (2020) highlights the potential of the presented techniques to equip computer system managers and operators for informed decision-making regarding system vulnerabilities. In their study, Hnamte et al. (2023), prioritize the development of hybrid machine-learning techniques as a means to effectively address the challenges associated with detecting complex attacks. The goal of combining algorithms is to increase performance. Moreover, researchers Ortega-Fernandez et al. (2023) note that, by developing adaptive systems, ML approaches enable cybersecurity professionals to proactively detect attacks and improve defense mechanisms. However, traditional ML challenges: According to Jayalaxmi et al. (2022), there are three types of machine learning techniques: supervised, unsupervised, and reinforcement learning. Real-world traffic data that is complex and noisy presents challenges for conventional methods. Finally, click fraud detection using intelligent techniques ML and DL is a hot topic in the current literature, with many studies using real-world click fraud datasets and advertising campaign access details for analysis (Aljabri and Mohammad, 2023) to draw conclusions.

In conclusion, a wide range of ML techniques are used in the context of cybersecurity to tackle the difficult problems of threat detection, response, and classification. These strategies cover supervised learning as well as more complex techniques like deep learning and ensemble learning, each with specific advantages for dealing with various cybersecurity scenarios.

2.6.3 RQ3. ML techniques in the field of cybersecurity face several challenges

The systematic literature review found that while ML and DL provide great performance in cybersecurity, they are not immune to errors, and some of these errors may incur higher costs than traditional cyber defence approaches (Zhang et al., 2022). However, the prevalent challenges found in current machine learning-based solutions are comprehensively outlined in the research of Vinayakumar et al. (2019). Moreover,

Siddiqi and Pak (2022) underlined that it is widely accepted that ML-based NIDS are superior at thwarting cyberattacks on computer networks. However, they face substantial challenges in maintaining their efficiency and efficacy in the face of always developing network threats. Nevertheless, Liang et al. (2019) stated that ML models in cybersecurity can only function well if they have access to timely, high-quality data. In addition, the constant and dynamic nature of data streams makes on-the-fly verification difficult, despite their value for enabling real-time detection. According to Fernandez De Arroyabe et al. (2023) examine the complexities associated with determining the appropriate allocation of financial resources towards cybersecurity solutions. Business enterprises have challenges when attempting to integrate resource allocation with security demands. Traditional approaches to cybersecurity are often characterized by their reliance on static rules and limited automation, as highlighted by Shaukat L., et al. (2020). This could potentially lead to inadequate responses in the face of transformative threats. Moreover, the issue of effectively adapting ML models to new vulnerabilities is emphasized by Seo et al. (2021). Models that are constructed based on previous data may encounter challenges when attempting to apply their learned knowledge to innovative attack techniques and patterns. In addition, the concept of interpretability is of significance. The importance of comprehending the decision-making process of machine learning models in the context of cybersecurity is emphasized by Bagaa et al. (2020). In order to establish trust and facilitate informed decision-making, it is imperative that the subject matter be comprehensible. However, as Kim and Pak, (2021), highlight, real-time packet processing presents a significant challenge for many machine learning-based security solutions. This difficulty arises from the fundamental characteristics of algorithms and the peculiarities of the data involved. Additionally, according to Liu et al. (2021) and Park et al. (2023) overfitting is a phenomenon that occurs when a model performs satisfactorily on the training dataset but is ineffective at generalizing to new data. In order to mitigate this problem, the attribute of robustness plays a pivotal role. Nonetheless, The researchers Latif et al. (2022) highlight the challenges associated with deploying machine learning models that are resource-efficient in environments characterized by constrained resources, such as Internet of Things (IoT) devices. The application of machine learning in the field of cybersecurity requires thorough data preparation, as stated by Sarker (2022). The presence of inadequate data quality can pose challenges during the deployment process. However, as Leevy et al. (2021) pointed out, the issue of data imbalance

presents difficulties. Inadequate minority class data could result in biased model performance. Nevertheless, according to the study conducted by Koay et al. (2023), it has been observed that widely used datasets such as KDDCup'99 and NSL-KDD have become outdated and unrealistic. This is a challenge for models aiming to accurately represent current cyberattacks. Aloraini et al. (2022) and Ferreira et al. (2023) have highlighted the vulnerability of ML models to adversarial attacks, in which malicious actors manipulate input data to undermine the model's functionality. Furthermore, the need to utilize training data of good quality, devoid of abnormalities, to ensure the successful performance of machine learning models is highlighted by Repetto et al. (2021) in their study on data quality for training. Moreover, the issue of detecting fraudulent actors inside the chain is pointed out by the researchers. According to Sarker et al. (2020), the success of machine learning models is greatly influenced by feature engineering, a process that can be difficult due to the complex structure and presence of clutter in cybersecurity data. In addition, the issue of unbalanced datasets and their impact on intrusion detection is examined by Abdelkhalek and Mashaly (2023). ML algorithms may not effectively learn patterns related to minority classes. However, the significance of feature engineering and selection for dependable machine learning models is highlighted by Disha and Waheed (2022). Cybersecurity data can be complex and cluttered, making this process more difficult. Nevertheless, Ahmad et al. (2021) highlight several challenges associated with supervised learning in the field of cybersecurity. These challenges include the acquisition of labeled data, managing inconsistent data representations, and the issue of overfitting. However, Zhang et al. (2022) highlight the importance of AI techniques, including Machine Learning and Deep Learning algorithms, in the supply of intelligent cybersecurity services and management.

In summary, machine learning approaches in the field of cybersecurity encounter various challenges and limits, including but not limited to concerns regarding data quality, adaptability to emerging threats, resource constraints, interpretability of results, susceptibility to adversarial attacks, and the handling of imbalanced datasets. The aforementioned challenges underscore the imperative for continuous research and development in order to overcome these barriers and enhance the efficacy of machine learning-based cybersecurity solutions.

2.6.4 RQ4. ML techniques in the field of cybersecurity are using a variety of metrics and evaluation methodologies

According to the findings, various criteria have been utilized to evaluate the performance of machine-learning techniques in the detection of attacks. The key metrics for evaluating detection performance are extensively detailed in the work of KhraISAt et al. (2019) and Pu et al. (2021). However, researchers Chakir et al. (2023) came up with a full set of well-known evaluation criteria to compare single and ensemble learning classifiers for detecting web-based attacks. Moreover, in their study, the researchers Aljabri and Mohammad (2023) employed four evaluation metrics to evaluate the overall performance of the intelligent models, the researchers justified the selection of these metrics based on their common usage in the existing literature. Nevertheless, Almashhadani et al. (2020), Campos et al. (2022), and Vinayakumar et al. (2019) have emphasized several binary classification metrics, including accuracy, false positive rate (FPR), precision, recall, and F1 score among others. In binary classification problems, these metrics evaluate the efficacy of trained machine learning models. The precision metric, however, is mentioned by Prazeres et al. (2023), and it measures how well a classification model can correctly identify affirmative cases. In addition, Bertoli et al. (2021) highlight the need to use evaluation metrics including accuracy, F1 score, precision, and recall to evaluate trained models. Both precision and recall are indicators of how accurate a model is. Nonetheless, Shaukat et al. (2020), provide a thorough description of these definitions, and they are crucial when evaluating machine learning techniques in the cybersecurity field. Notwithstanding, the confusion matrix relies on these to perform its assessment of a classification system. Accuracy, true positive rate (TPR), false positive rate (FPR), and F-measure are often used metrics for evaluating the success of machine learning systems in cyber security, as stated by Lee et al. (2019). Furthermore, accuracy, true positive rate (TPR), false positive rate (FPR), and F-measure are highlighted as regularly used metrics for evaluating the efficacy of machine learning systems in cybersecurity by Latif et al. (2022) and Lee et al. (2019). However, area under the curve (AUC) investigated by Leevy et al. (2021), Siddiqi and Pak (2022) define the traditional F1-score, ROC curve, and AUC as important metrics used to evaluate machine learning models on imbalanced data. In addition, accuracy is a widely used metric for evaluating model performance across domains, as Ahmad et al. (2021) note.

Furthermore, metrics from the Confusion Matrix: False Negatives, False Positives, True Negatives, and True Positives are described by Liu et al. (2021). True positive (TP), false positive (FP), true negative (TN), and false negative (FN) are major factors in the confusion matrix, which allow for the calculation of selected metrics for classification tasks, as explained by Yong and Gao (2023). Moreover, Abdelkhalek and Mashaly (2023), in their article "Confusion Matrix Terminology," define the terms true positives (TP), false negatives (FN), true negatives (TN), and false positives (FP) that appear in the confusion matrix used to assess the accuracy of the model. However, Koay et al. (2023) stresses the significance of metrics for evaluating the success of attack detection strategies in recognizing and labeling attacks, and how erroneous metrics can lead to biased evaluation.

In conclusion, a variety of metrics and methodologies are employed to evaluate the performance of machine learning techniques in cybersecurity. Accuracy, precision, recall, and the F1 score are just a few examples of the many metrics used in machine learning and data science.

2.6.5 RQ5. The Utilization of Supervised Learning Techniques in the Field of Cybersecurity

According to the SLR findings, supervised learning techniques are of significant importance in diverse cybersecurity domains as they contribute to the detection and mitigation of security vulnerabilities. However, they also come with drawbacks and vulnerabilities. The results obtained from this study suggest that supervised learning algorithms, specifically KNN, Decision Trees (DT), and Naive Bayes (NB), exhibit a significant ability to accurately detect web attacks (Chakir et al., 2023). Additionally, the reasoning behind taking these algorithms into account is that they use various methods of developing smart models (Aljabri and Mohammad, 2023). Moreover, Aloraini et al. (2022) added that supervised machine learning models like DT, RF, NB, and SVM were used to identify DoS attacks in the context of an Internet of Things (IoT) smart home network. However, researchers suggested utilizing supervised learning techniques in the field of intrusion detection (Kosmanos et al. 2020; WISAnwanichthan and Thammawichai 2021), this approach involves the classification of network activity into two categories: normal and malicious. By employing this method, possible threats can be identified in real time. This

phenomenon facilitates the prompt identification of security issues. In addition, behavior anomaly detection involves the utilization of supervised learning to analyze labeled data to discover patterns of abnormal user behavior. These patterns can serve as indicators of potential insider threats or unauthorized efforts to gain access (Lee et al., 2019; Park et al., 2023). The function of this system is to establish a standard for typical conduct and identify any deviations from it. Nonetheless, the detection and classification of malware can be effectively achieved through the use of supervised learning models, which have demonstrated a high level of proficiency in this task. This capability enables the timely identification of malware, allowing for fast implementation of mitigation measures (Sarker, 2022). Notwithstanding, Pu et al. (2021) underline that SVM, a supervised learning model renowned for its pattern recognition capabilities, is utilized for data analysis. Additionally, OCSVM, an extension of the SVM approach, exhibits particular suitability for unlabeled data. Nevertheless, it is imperative to recognize the potential risks linked to these approaches. However, Almashtadani et al. (2020) highlight the importance of dataset quality in supervised learning for efficient domain generation algorithm (DGA) detection. Furthermore, pattern classification is a prominent field within the domain of cybersecurity, with a particular focus on supervised machine-learning techniques (Ezugwu et al., 2023). Classical and quantum learning algorithms have been specifically developed to address this domain and to extend or augment traditional methodologies. Moreover, classification and regression are considered the two main categories of supervised learning methods, as stated by Liang et al. (2019) and Sarker et al. (2020). These predictive models are utilized to forecast the results of specific security events, such as denial-of-service assaults and various network invasions.

4.1.5.1 Limitations and Weaknesses of Supervised Learning in Cybersecurity.

The SLR found that despite the efficacy of supervised learning approaches in the field of cybersecurity, there are several obstacles and weaknesses that impede their optimal performance. One of the major obstacles to achieving successful supervised learning is the difficulty in obtaining extensive and representative labeled datasets (Prazeres et al., 2023). The limited availability of high-quality data might impede the process of training models, especially when it comes to new risks. Moreover, the literature has thoroughly explored a variety of supervised learning techniques, each offering its own set of strengths and limitations, which can be expanded upon in the study conducted

by KhraISAt et al. (2019). According to Bland et al. (2020), for a supervised learning method to function properly, a suitable training dataset must be available. Without access to such information, the agent must rely on its own prior experiences. However, Bagaa et al. (2020) shed light on how the resource requirements of supervised learning models can have an impact on their practicality in real-time applications. In many instances, a significant amount of computational resources is necessary, a circumstance that may present challenges in certain settings where such resources may not be readily accessible. According to Sarker (2022), “adversarial attack”: The presence of adversarial attacks presents a significant concern for models that rely on supervised learning. The manipulation of input data by attackers might result in the deception of the model, ultimately yielding inaccurate outcomes (Aloraini et al., 2022). The existence of this vulnerability gives rise to apprehensions regarding the dependability of security solutions that are based on machine learning. Moreover, Leevy et al. (2021) highlighted that “overfitting” is a prevalent concern encountered in the realm of supervised learning when models exhibit satisfactory performance on the training dataset but demonstrate subpar performance when applied to unseen data. Achieving a suitable equilibrium to prevent overfitting is a critical obstacle. However, imbalanced datasets, characterized by a substantial disparity in the number of cases between different classes, have the potential to introduce bias into models (Koay et al., 2023). Maintaining equitable class representation is crucial to mitigating the potential for biased outcomes. Notwithstanding, the detection of zero-day vulnerabilities poses a challenge for supervised learning algorithms because of their dependence on historical data for training (M. R. et al., 2021). The ever-changing nature of the threat landscape poses a persistent and enduring challenge.

To summarize, supervised learning methods provide useful answers in the field of cybersecurity, including many applications like as intrusion detection, behavior anomaly detection, malware identification, and pattern categorization. Nevertheless, it is imperative to acknowledge and tackle many obstacles that arise in the context of machine learning models. These challenges encompass data labeling, resource allocation, adversarial attacks, overfitting, imbalanced datasets, and zero-day vulnerabilities. Addressing these issues is of utmost importance to improve the effectiveness and security of these models when applied in real-world scenarios. There is a need for future research to prioritize the enhancement of the resilience of

supervised learning models to effectively address the dynamic requirements of the cybersecurity field.

4.1.6 RQ6. Unsupervised learning techniques for cybersecurity

The SLR found that unsupervised learning methods provide significant contributions and anomaly detection skills within the field of cybersecurity, particularly in situations where there is limited availability of labeled data (Kandhro et al., 2023; Pu et al., 2021; Vinayakumar et al., 2019). These techniques independently identify and analyze patterns and structures inherent in the given dataset. However, unsupervised learning techniques are of great importance within the field of cybersecurity, specifically in the evaluation of performance and the analysis of unlabeled data (Khraisat et al., 2019). In the research they conducted, Chakir et al. (2023) undertook an investigation to evaluate the efficacy of different machine learning methods, encompassing both supervised and unsupervised techniques, within the domain of anomalous attack detection.

The utilization of unsupervised clustering methods, such as k-means and DBSCAN, enables the grouping of interconnected data points by their qualities. This characteristic renders these techniques valuable in the identification of patterns within network traffic, user behavior, and system data (WISAnwanichthan and Thammawichai, 2021). However, the utilization of unsupervised learning techniques in the field of cybersecurity enables specialists to enhance their comprehension of the fundamental structure and patterns within data, even when the data lacks explicit labels (Bagaa et al., 2020). Moreover, the utilization of clustering algorithms enables the identification of potential clusters of cyber threats or atypical behaviors that may not be readily apparent in labeled data, hence offering a valuable means for detecting threats (Ezugwu et al., 2023). Furthermore, autonomous anomaly detection is a form of unsupervised learning that involves the utilization of autoencoders and clustering techniques (Liang et al., 2019). This approach enables the autonomous identification of anomalies and abnormalities from established behavioral patterns. By doing so, it presents a viable alternative to conventional methods of threat detection, as highlighted by Repetto et al. (2021). Moreover, a range of unsupervised techniques exists within the field of unsupervised learning. These techniques include autoencoders (such as SpAE, UAE, and VAE), Fair Clustering, Isolation Forest, and OneClass Support

Vector Machine (OCSVM). These methods can automatically classify abnormal data as "attacks" without the need for human intervention, (Koay et al., 2023).

According to M. R. et al. (2021), challenges of False Positives: While unsupervised learning can detect new attacks, it may come with a higher rate of false positives, making it crucial to pinpoint the source of anomalies. Moreover, Ahmad et al. (2021), highlighted, Class Imbalance: In supervised learning, class imbalance can lead to biased model performance. The issue can be addressed by employing unsupervised learning approaches, which do not depend on labeled classes. Moreover, anomaly detection in the field of cybersecurity often involves the utilization of unsupervised learning techniques, such as Autoencoders. These approaches are employed to develop models that are capable of identifying anomalies by establishing patterns of normal behaviour (Ortega-Fernandez et al., 2023). Further, the analysis of raw data using unsupervised learning methods involves the examination of unprocessed and unlabeled data. This process aims to uncover patterns that were previously undiscovered by employing data reduction and clustering techniques such as K-Means and Principal Component Analysis (PCA) (Jayalaxmi et al., 2022).

The findings mentioned above highlight the adaptability and effectiveness of unsupervised learning techniques in the context of cybersecurity, namely in the areas of pattern identification, anomaly detection, and comprehension of data structures derived from unannotated data.

4.1.7 RQ7. Utilization of Deep Learning in Cybersecurity

According to the research findings revealed that recently, there has been an evaluation of the application of Deep Learning (DL) approaches using various neural networks to identify different attacks in various contexts, (Campos et al., 2022). In addition, Vinayakumar et al. (2019) highlighted that DL algorithms, including CNNs, RNNs, and Long-Short Term Memory (LSTM) networks, are utilized in the field of intrusion detection. According to Zhang et al. (2022), the algorithms possess the capability to automatically extract complex properties from unprocessed data, rendering them well-suited for the detection of sophisticated and dynamic cyber threats. However, the relevance of ensuring the stability of deep learning models in edge computing infrastructures cannot be overstated, Liang et al. (2019) emphasize the necessity of implementing error-recovery strategies in distributed machine-

learning systems. Furthermore, the implementation of deep learning networks serves as a crucial factor in efficiently addressing unforeseen and unpredictable cyber-attacks. Nevertheless, the capacity of deep learning to autonomously acquire hierarchical representations from data makes it very suitable for managing complex and high-dimensional cybersecurity datasets. According to Lee et al. (2019), this characteristic enhances its efficacy in detecting anomalies and recognizing patterns related to cyber risks. Furthermore, Deep neural network techniques such as Auto-encoders, Generative Adversarial Networks (GANs), and Deep Belief Networks (DBNs) are commonly employed in the field of cybersecurity to facilitate unsupervised and generative learning tasks. According to Sarker, (2022), the utilization of these techniques can be beneficial in the identification of anomalies as well as in the creation of authentic synthetic data for training.

4.1.7.1 The Benefits of Deep Learning in the Field of Cybersecurity.

The result found that the utilization of deep learning techniques enables the automatic extraction of complex features from raw data, rendering them well-suited for complicated and high-dimensional cybersecurity datasets.

Deep learning algorithms provide superior performance compared to typical machine learning approaches in the context of handling significant amounts of security data. According to Latif et al. (2022), they demonstrate exceptional performance in situations that require the processing of a large amount of data. Further, deep neural networks, including CNNs and RNNs, possess sophisticated learning mechanisms that allow them to effectively capture complex patterns and time-dependent connections within cybersecurity data (Hnamte et al., 2023). Moreover, deep learning methods frequently demonstrate superior levels of accuracy in comparison to traditional machine learning models, particularly when applied to complex tasks such as image identification, natural language processing, and intrusion detection, (Siddiqi and Pak, 2022; Zhang et al., 2022). Nevertheless, Park et al. (2023) highlighted that deep learning algorithms have been found to exhibit sensitivity towards environmental changes.

4.1.7.2 The Limitations of Deep Learning in the Field of Cybersecurity.

According to the research findings, deep learning models require a considerable volume of data to undergo effective training. Although standard machine learning

models might show satisfactory performance when dealing with smaller datasets, deep learning models demonstrate superior performance when confronted with larger and more diversified datasets, (Shaukat et al. 2020). Moreover, the process of training deep learning models may present significant computing demands and consume a substantial amount of time, necessitating the utilization of specialist hardware or cloud-based resources as (Vinayakumar et al., 2019) noted. Furthermore, the concept of interpretability pertains to the difficulty in understanding the decision-making process and rationale behind specific predictions made by deep learning models. This challenge arises from the intricate nature of their architectures, which sometimes leads to these models being perceived as "black boxes," (Aljabri and Mohammad, 2023). According to Kandhro et al. (2023), overfitting is a common issue encountered in deep learning models, particularly when the available training data is limited or contains noise. To address this issue, it is necessary to employ regularization approaches and engage in thorough hyper-parameter tuning.

In conclusion, deep learning methodologies have notable benefits in effectively managing complex cybersecurity data and attaining a commendable level of precision in tasks such as intrusion detection and threat identification. Nevertheless, these methods necessitate significant amounts of data and processing resources, potentially resulting in a lack of interpretability when compared to traditional machine-learning approaches. The selection between deep learning and traditional techniques is dependent upon the particular cybersecurity objective, the accessibility of data, and the computational capabilities at hand.

4.1.8 RQ8. Utilization of Reinforcement Learning in Cybersecurity

According to the findings, Reinforcement learning (RL) has found several applications in the field of cybersecurity, each contributing to improving security measures.

One notable utilization of reinforcement learning in the field of cybersecurity is intrusion detection. Reinforcement learning techniques facilitate the ability of security systems to acquire knowledge from past data and current network traffic in order to detect abnormal patterns and potential security breaches (Liang et al., 2019). According to Bland et al. (2020), the adaptive characteristic of reinforcement learning enables these systems to consistently revise their models and adjust to changing attack

techniques. Consequently, this capability enhances the precision and effectiveness of intrusion detection. However, the application of RL in the development of intelligent agents for network security enables the detection and prevention of breaches within computer networks. Reinforcement learning agents acquire knowledge by retrospective analysis of prior experiences and engagements with the surrounding environment, hence enhancing their ability to discern recurring patterns and detect deviations indicative of malevolent behaviors. According to Shaukat et al. (2020), this phenomenon results in enhanced precision and effectiveness of intrusion detection systems. Moreover, the RL techniques contribute to the development of defense systems that are proactive and flexible. Security systems integrated with reinforcement learning have the ability to anticipate probable attack scenarios by leveraging knowledge gained from adversarial encounters. The capacity to predict potential threats enables systems to take proactive measures in order to increase their overall security posture, (Liu et al., 2021). Notwithstanding, improved resource allocation is a crucial aspect in the field of cybersecurity, and reinforcement learning has emerged as a promising approach to achieve this objective. RL algorithms have the capability to inform decision-making processes related to the distribution of security resources, such as processing power and bandwidth, by leveraging insights gained from past data and interactions. According to Sarkar et al. (2022), the optimum utilization of resources is crucial in countering future threats. Furthermore, the utilization of RL in the field of cybersecurity has been found to enhance the efficacy of decision-making procedures. According to Ezugwu et al. (2023), systems that utilize reinforcement learning have the ability to acquire knowledge from previous actions and their corresponding results. This capability enables these systems to make improved decisions in real-time when it comes to mitigating threats and responding to incidents.

4.1.8.1 The Benefits of Utilising RL in the Field of Cybersecurity.

According to the findings, the concept of adaptability in the realm of cybersecurity refers to the ability of systems to adjust and respond to evolving attack techniques and emergent threats. The adaptive nature of the learning process enables the continued effectiveness of defence systems, even when confronted with developing means of assault, (Bland et al., 2020). Additionally, the utilization of RL in security systems allows for a proactive defence approach, wherein the systems are capable of anticipating potential attacks and implementing preventive actions. The

implementation of a proactive approach aids in the mitigation of potential threats before their manifestation and subsequent damage as noted by Ezugwu et al. (2023). Moreover, the use of resources in an efficient manner is achieved through the implementation of RL, which optimises the allocation of security resources by directing them to areas where they are most essential. As a consequence, there is an enhancement in resource allocation and an overall improvement in system performance, (Sarkar et al., 2022).

Continuous improvement is a key characteristic of RL-enabled systems, as they possess the ability to continually learn and enhance their performance over time. This ongoing learning process enables these systems to become progressively more effective in tasks such as threat identification, prevention, and response.

4.1.8.2 These parts outlines limits and cautions of RL findings.

According to Bagaa et al. (2020), a thorough understanding of the fundamental algorithms and their appropriate setup is necessary for the successful implementation of reinforcement learning approaches in the field of cybersecurity. Nevertheless, the training data to achieve optimal performance in reinforcement learning, it is imperative to have access to comprehensive and relevant training data. According to Sarker (2022), the lack of suitable training data can hinder the knowledge-acquisition process. Furthermore, in the study conducted by Liu et al. (2021), the phenomenon of model overfitting refers to a situation when a statistical model is excessively tailored to suit the training data, resulting in The development of overfitting is a possible issue in the training of RL models, particularly when the training data demonstrates bias or inadequately represents real-world conditions. Furthermore, in the study conducted by Sarker et al. (2020), computational resources are often required to support the training and execution processes of RL methods, as they can be highly computational.

In summary, reinforcement learning offers considerable potential in the field of cybersecurity, including many applications such as intrusion detection and resource allocation optimization. The tool's adaptability, proactive skills, and capacity for effective decision-making render it a significant asset in enhancing security measures within a dynamically changing threat landscape. Nevertheless, it is imperative to thoroughly deliberate on the training data, algorithm complexity, and computer resources in order to achieve a good implementation.

4.1.9 RQ9. Emerging Trends and Approaches in the Evaluation of ML Techniques for Cybersecurity

The findings of the SLR indicated that the utilization of adversarial machine learning algorithms has seen a rise in evaluating the resistance of cybersecurity models against complex attacks. According to Aloraini et al. (2022), these strategies test models using adversarial inputs to determine how durable and flexible they are. However, there is an emerging inclination towards the creation and advancement of cybersecurity-specific benchmarks and statistics. The primary objective of this endeavor is to facilitate balanced evaluations of various methodologies and improve the reproducibility of findings. The benchmarks provided by Shaukat et al.(2020), serve the purpose of evaluating the performance of machine learning models inside actual cybersecurity contexts. Notwithstanding, the integration of real-time and streaming data analytics capabilities into the performance evaluation process is gaining significance due to the rapid growth of cybersecurity threats. According to Liang et al. (2019) the significance of tackling the time and computational demands involved with training techniques is emphasized by recent developments in evaluations of machine learning. Moreover, as noted by Latif et al. (2022), there is a growing trend in the field of cybersecurity to investigate the utilization of hardware acceleration as a means to improve the performance of various procedures. An example of enhancing the effectiveness of cyberattack detection can be observed by the integration of deep learning algorithms with accelerators based on field-programmable gate arrays (FPGAs). Nevertheless, researchers are now investigating the utilization of alternative classifiers and methodologies to enhance the effectiveness of classification. The study by Leevy et al. (2021) involves the evaluation of classifier performance using different network intrusion detection datasets. Additionally, the researchers explore several ways to mitigate the issue of class imbalance. However, future research endeavors are currently dedicated to the integration of a more extensive array of attack types within the framework of the design and evaluation of detection technologies. According to this measure promises the efficacy of the models to detect a wider variety of threats within a dynamic cybersecurity environment. Furthermore, Park et al. (2023) emphasized that it is essential to adopt an integrated approach that integrates many technologies, moving beyond reliance on individual methodologies like statistical analysis or machine learning and deep learning techniques, in order to overcome the limits identified in current IDSs. In order to boost the performance evaluation of

machine learning in IDS, (Vinayakumar et al., 2019) propose the utilization of upgraded hardware and the implementation of intricate DNN architectures trained through distributed approaches.

The current trend in evaluation metrics is shifting towards a more complete approach that goes beyond the conventional accuracy-based measures. Scholars are placing significant emphasis on incorporating scalability, time and processing costs, reliability, and other pertinent elements to achieve a greater understanding of the performance of a given technique, Koay et al. (2023). Moreover, the utilization of ensemble learning and transfer techniques has emerged as a novel strategy in the field, wherein many models are combined to enhance the overall performance of a system. Furthermore, the exploration of transfer learning approaches is being conducted to repurpose and modify models that have been trained for a specific application, to address novel forms of threats or diverse domains within the context of cybersecurity. Furthermore, the integration of reinforcement learning is being employed in the development of intelligent and self-enhancing cybersecurity systems. The aforementioned methodology enables security measures to autonomously adjust to evolving threat environments by acquiring knowledge from interactions with the surrounding environment, (Disha and Waheed, 2022). According to Hnamte et al. (2023) the primary focus lies in the quality of training data when evaluating the effectiveness of machine learning techniques in the field of cybersecurity. By utilizing training data of superior quality, algorithms can improve their analytical and predictive capabilities, thereby facilitating more informed decision-making in subsequent endeavours. Moreover, there is ongoing work in the development of visualization tools and interactive incident diagrams to improve analysts' effectiveness and offer more comprehensive depictions of security warnings and occurrences (Ferreira et al., 2023).

In conclusion, the evaluation of machine learning methods in the domain of cybersecurity is currently experiencing a transition towards adversarial evaluation, the establishment of specific benchmarks, the utilization of real-time analytics, the incorporation of hardware acceleration, and the adoption of holistic metrics. The utilization of various classifiers, ensemble learning methodologies, transfer strategies, and the integration of reinforcement learning are increasingly being seen. The primary objective of these approaches is to effectively tackle the ever-changing cybersecurity

concerns and implement security solutions that are more precise, effective, and adaptable.

4.2 Source of Data

Table 4.1 presents a detailed overview of the retrieved material and significant findings obtained from the papers evaluated in the study. The systematic literature review provides a significant resource for readers and researchers who require a quick reference to the fundamental ideas and outcomes obtained from the review. This table condenses complex information into a structured format, facilitating an efficient understanding of the research landscape and the contributions of the selected articles. Each entry in **Table 4.1** represents a distilled essence of the respective article, making it a vital reference for anyone interested in gaining insights into the field of study covered in this review.

Table 4.1
Presents the extracted information from the articles

Reference	Identification of Gaps	Challenges and Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps. of unsupervised and limits of DL	Improving security RL	Future directions	Key findings
Bland et al. (2020)		ML can help computer system defenders identify vulnerabilities and their chances of being exploited. Computer hackers can design assaults using ML.		The availability of a training set is essential to the success of any supervised learning algorithm. Without a data set to model, a learning agent is left to rely on its own observations.		RL is used in intrusion detection in cybersecurity. Security systems can detect anomalies and threats in historical data and real-time network traffic using RL algorithms.		Reinforcement learning has been widely used in cybersecurity to increase security. These methods improve advanced cyber threat detection, prevention, and response.
Almashhadani et al. (2020)			Several binary classification metrics, including accuracy, FPR, precision, recall, and F1 score, were utilized to assess the performance of the trained ML models.	MaldomDetector, an ML-based detection system, trained and evaluated on a high-quality pre-labeled ground truth dataset of malicious and benign data, demonstrating the importance of dataset quality in supervised learning for efficient DGA detection.				An ML-based detection method that uses character-level information from the DNS request's domain name string to achieve 98% detection accuracy and a 4% false positive rate.
Prazeres et al. (2023)			The precision metric, which assesses the classification model's accuracy, is one of the often employed metrics.	Obtaining big labeled datasets that are representative of the phenomenon being studied is a significant obstacle to overcome when utilizing Supervised Learning.				When evaluating the performance of a model, it is extremely important to make use of appropriate metrics
Arroyabe et al. (2023)	ML encompasses a set of computational algorithms that by learning from existing data can perform pattern identification, classification, and prediction	Finding the appropriate degree of investment in cybersecurity technologies is one of the biggest difficulties that enterprises face today.		The architecture that multilayer perceptron applications have employed is referred to be a supervised network since the projected outcomes may be tested against values for the dependent variables that are known.				
Aloraini et al. (2022)	There has been an increase in the application of adversarial machine learning techniques to assess the robustness of cybersecurity models against sophisticated attacks.			In the domain of IoT smart home networks, the utilization of supervised ML algorithms such as DT, RF, NB, and SVM was employed to detect instances of DoS assaults.				IoT-based ML systems are vulnerable to degraded performance from ML-based IoT threatening insiders if their systems are in comparison to adversarial assaults is not taken into account.

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps of unsupervised	Benefits and limits of DL	RL to improve security	Future directions	Key findings
Kosmanos et al. (2020)		The detection mechanism of the suggested IDS relies on the utilization of various ML techniques, including RF and k-NN, employing metrics in a cross-layer methodology.			Both supervised learning techniques, namely k-NN and RF, enjoy significant popularity in the field.					The PVRS system evaluates the proximity between two communicating nodes by comparing the distances obtained from their onboard Units with the estimated distance derived using the Δu value.
Campos et al. (2022)	It is possible that the whole scope of cyber risks in IoT contexts is not captured by datasets like N-BalIoT and MedBlIoT, which focus on specific attacks related to IoT device botnets.	The utilization of ML methodologies in IDS has received significant attention, with several approaches being explored, including neural networks and clustering algorithms.					DL techniques have recently been explored in such settings using various types of neural networks for the identification of various assaults.			Outcomes demonstrate that an instance selection approach based on the Shannon entropy of each local dataset can improve accuracy while producing similar results compared to balancing the dataset among both sides.
Chakir et al. (2023)				These metrics, commonly used in the literature, cover various aspects of classifier performance, ensuring a thorough assessment of their effectiveness.	Cybersecurity has gained knowledge in threat detection using supervised techniques like KNN, Decision Tree and Random Forest.	Unsupervised learning is vital in cybersecurity, notably for performance evaluation and unlabeled data processing.				A single classifier or ensemble technique for web application security depends on the application, according to the study.
Aljabri and Mohammad (2023)	Detecting various forms of attacks with the use of AI methods like ML and DL is a rapidly growing field of study.			The overall efficiency of the smart models was metrics across four different dimensions.	ML methods like DT, SVM, NB, Ripper, PART, NN, and RF. Consider these algorithms because they generate intelligent models uniquely.		Interpretability refers to the difficulty of understanding DL model predictions' decision-making process and reasoning. Their intricate architecture makes this difficult.			All algorithms tested gave positive results, proving the study's features' usefulness.
Bertoli et al. (2021)	Using obsolete datasets for network security research is generally acknowledged to be difficult. The most-used datasets are over two decades old, which worries academics			ML domain uses accuracy, F1-score, precision, and recall as assessment metrics for selecting trained models, with precision representing exactness and recall completeness.						training ML models, realizing (implementing) the solution in a target machine, and evaluating the performance of the protection module are the steps in this process.

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps of unsupervised	Benefits and limits of DL	RL to improve security	Future directions	Key findings
Zhang et al. (2022)		AI methods like ML and DL algorithms have improved cybersecurity services and applications in recent years.	A number of costly mistakes can be made by Mal. and DL algorithms, despite their otherwise excellent performance.				Several cybersecurity domain applications could benefit from the excellent results that ML and DL algorithms can achieve on benchmark datasets.			Despite the remarkable performance of DL algorithms, they are not error-free and occasionally make mistakes that are more costly than traditional cyber security strategies.
Shaukat et al. (2020)	Researchers need new automated security solutions to solve security problems. Best practice: automated ML to detect emerging cyber risks.	In the field of ML, the SVM is often regarded as the most popular and successful technique for IDS.	Traditional ML methods lack automation and control devices statically via network security rules.	The following metrics— True Positives, True Negatives, False Positives, and False Negatives—are used to evaluate cybersecurity ML algorithms.			Classical ML models performed better on smaller datasets. On larger datasets, data-hungry deep learning algorithms perform well.	Intelligent agents with the ability to recognize and stop breaches in computer networks can be made via RL.	Cybersecurity model defense against sophisticated attackers is increasingly evaluated using adversarial ML techniques.	ML may help respond quickly to cyberattacks. These difficulties are addressed with ML methods since they can swiftly respond to new threats and learn from prior mistakes.
Seo et al. (2021)	Modern approaches to determining the efficacy and dependability of ML applications for cybersecurity	NIDS has adopted ML techniques including SVM, RF, and k-NN. These algorithms help cybersecurity systems classify network threats.	ML models trained on previous data may not generalize to new cyber threats.							A neural detector called MHSA was introduced to fix the issues. Its multi-head self-attention technique is excellent at gathering irregular network traffic evidence.
WIS Anwanichthan and Thammawichai (2021)		ML algorithms are unique. Recent approaches use two or more learning algorithms to better recognize distinct threats.			Supervised learning allows IDS to classify network activity as normal or malicious, enabling real-time threat detection.	Unsupervised clustering techniques such as k-means and DBSCAN combine related data points based on their attributes.				Single ML models have a low detection rate, especially for rare attacks, because they are not effective in identifying all forms of attacks...
Lee et al., (2019)	Many AI and ML methods have tested outdated datasets. This complicates performance evaluations.	One of the biggest cybersecurity concerns is automating and improving cyber threat detection.		In cybersecurity, accuracy, TPR, FPR, and F-measure are the most common metrics for evaluating ML systems.	Supervised learning can recognize atypical user behavior that may suggest insider threats or unauthorized access.		DL technique has been greatly advanced in many areas and is still ongoing in many industries beyond an area of ML that applies			Security analysts can efficiently handle important warnings by condensing large-scale data into event profiles using DL for cyber-threat detection

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps of unsupervised	Benefits and limits of DL	RL to improve security	Future directions	Key findings
Bagaa et al. (2020)	IoT will soon change our lives. Cybersecurity attacks are skyrocketing, and on-demand security is a breakthrough.	Many ML techniques are used by AI-based reaction agents to identify IoT and network intrusions.	Understanding the thought process that goes into ML model decisions is necessary in the field of cybersecurity.		To overcome supervised learning's limits and weaknesses in cybersecurity, more robust ML model validation, and data pre-treatment methods must be developed.	Unsupervised learning helps cybersecurity experts grasp unlabeled data's structure and trends.		In cybersecurity, RL focuses on examining problems and strategies that attempt to enhance its model.		Traffic can drain energy and CPU, lowering device usability. Alternative IoT security uses machine learning methods.
Kim and Pak, (2021)	The most important performance evaluation factor is attack detection speed. Speed must be much faster than real-time detection.		Most ML-based security solutions struggle with real-time packet processing due to algorithm and network data features. F1-score.	Machine learning algorithms in cybersecurity are evaluated using measures including accuracy, recall, and F1-score.						Their methods primary benefit is protecting ML benefits while processing massive traffic volumes quickly. Cybercrime is rising, yet networks and people may be protected.
Liu et al., (2020)			Machine learning models must be robust to avoid overfitting and succeed with new data.	The cybersecurity effectiveness of ML algorithms was evaluated using four criteria and assessment methods.	An outstanding supervised learning method, RF can train a model to predict a dataset's sample type based on its unique properties and classification results.		DL's ability to automatically extract features has helped computer vision, autonomous driving, and natural language processing advance.	Techniques for reinforcement learning aid in the growth of proactive and adaptable defense systems		This study found that DL outperforms ML after sampling the imbalanced training set using the "difficult set sampling technique".
Latif et al., (2022)	Future performance evaluations will need real-time and streaming data analysis skills to stay up with expanding cybersecurity risks.	Machine learning can help authorize and secure IoT environments.	Resource constraints Cybersecurity ML models must work in low-resource embedded and IoT systems. Model complexity and resource availability may conflict.	ML algorithms in cybersecurity are evaluated using accuracy, precision, recall, and F1 score.			DL-based algorithms extract patterns better than traditional learning methods, according to multiple research.		Hardware-wise, a DL, a dense random neural network, and an FPGA-based accelerator might increase cyberattack detection.	The model's experiments showed it outperforms other ML/DL approaches.
Young and Gao, (2023)	Combining models using ensemble learning to increase cybersecurity system performance and reliability.	IDSs can now detect zero-day and other new attacks owing to machine learning.		ML classification metrics may usually be calculated using the confusion matrix's output.						The study's algorithm-based model performs better. The proposed classification strategy of HFBHA with XGBoost benefits IDSs.

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps of unsupervised	Benefits and limits of DL	RL to improve security	Future directions	Key findings
Liang et al. 2019	ML and deep neural network design have given self-driving cars and sophisticated smartphone apps unequaled analytical powers.	The standard ML methodologies encompass supervised learning, unsupervised learning, and reinforcement learning approaches.	ML models require high-quality, timely input, which data streams give to enable real-time detection but are difficult to evaluate.		Supervised learning uses labeled datasets to train models. Classification and regression differ in goal label granularity.	Clustering, density estimation, and dimension reduction are unsupervised learning tasks.	Deep learning networks are essential for addressing unforeseen cyber threats.	Deep RL solved the cloud resource allocation problem adaptively.	ML methods cannot handle dynamic systems because training takes time and computing. New training data is created continuously for IDS.	This comprehensive research and debate show the benefits of using ML approaches to cybersecurity and Cyber-Physical Systems.
Sarker, (2022)		Types of learning algorithms supervised, semi-supervised, and RL are used to analyze cybersecurity data and provide unique safety services	Any modern cybersecurity program needs ML. Modern cybersecurity solutions are practically unachievable without ML. However, has challenges.		Adversarial attacks on supervised learning models manipulate inputs to meet their goals.	Unsupervised clustering methods like k-means and DBSCAN put together comparable data points based on their attributes.	Deep neural network techniques like Autoencoders, Generative Adversarial Networks, and Deep Belief Networks can address cybersecurity challenges.	Cybersecurity benefits from RL's adaptive and intelligent defense mechanisms, threat detection and prevention, resource allocation, and decision-making.		The study trains complex learning algorithms for intelligent decision-making and automation using real-world cyber data and target application knowledge.
KhraISat et al. (2019)	Many cybersecurity databases lack updated malware attack data, making them obsolete.	Machine learning has two main methods: supervised and unsupervised.		There are numerous classification metrics for IDS, some of which have multiple names	Supervised learning requires training a classifier to determine the link between input data and labeled output value.	Unsupervised ML uses unlabeled input data. Instead, learning automatically organizes data into classes.				A significant problem for this field of study is the creation of IDSs that can counter these evasion methods.
Leevy et al. (2021)	We should update the evaluation criteria for the detection accuracy-false positive rate trade-off to account for real-world false alarms	ML algorithms may have difficulty accurately learning patterns from the minority group, which can lead to biased model performance		Using a single performance metric to evaluate machine learning models on highly skewed datasets.	Overfitting, when a model performs well on training data but poorly on unseen data, reduces generalization.	Clustering evaluations can show cyber threat or deviant activity clusters that don't appear in labeled data			A new classifier and Destination_Port encoding could be considered in the future.	
Koayy et al. (2023)	Using adversarial ML to evaluate cybersecurity models against sophisticated attacks is an innovation.	Combining supervised and unsupervised learning procedures is possible in deep learning systems, which are ML types.	Rare, high-quality data sets for cybersecurity ML-based algorithm evaluation. The used datasets are outdated	Inadequate metrics can bias evaluation, affecting the approach's dependability and generalizability	The 'labels' or human interaction of supervised learning are what allow it to learn the patterns.	Unsupervised learning finds patterns without instruction. Insufficient labels in training data make this learning method desirable.	numerous processing layers DL aims to learn data representations with abstraction levels via "multiple processing layers."		Future research must include more attack types in detection technology design and evaluation to increase attack coverage and performance in changing environments.	Most ML algorithms have been evaluated against the ubiquitous cyberattack of fraudulent data insertion in Industrial Control systems, the study found.

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics	Vulnerabilities of Supervise Learning	Apps of unsupervised DL	Benefits and limits of DL	RL to improve security	Future directions	Key findings
Jayalaxmi et al. (2022)		The main machine learning methods are supervised, unsupervised, and reinforcement.			Supervised algorithms can train on class-labeled data and connect input and output units.	Unsupervised learning methods analyze raw data without first labeling it, revealing previously unknown patterns.	IDS models developed using DL techniques with amazing quality of self-learning are advantageous.		In cybersecurity, we need training data to assist algorithms in identifying patterns, predicting consequences, and making smarter decisions.	The performance of IDS has also been improved because of the application of ML and DL techniques.
Ezugwu et al. (2023)		Cybersecurity protects networks, systems, hardware, and data from computer attacks. Identifying risk trends using data analysis and ML can avert security breaches			Within the realm of supervised ML, one of the most significant positions to undertake is pattern classification.	Clustering performance evaluations can reveal security risks or anomalous activity clusters that labeled data may not disclose.		Cybersecurity benefits from RL's adaptive and intelligent defense mechanisms, threat detection and prevention, and resource allocation and decision-making.		ML is an area of AI that uses computer methods and learning algorithms to solve real-world problems.
Ferreira (2023)	ML has pros and cons like every tool. Recent studies and experiments have focused on cybersecurity and ML.		Adversarial attacks on machine learning systems can misclassify and jeopardize safety.							
Repetto et al. (2021)			One challenge of utilizing ML for cybersecurity is spotting adversarial or fraudulent individuals in the chain.			A bold threat detection option, unsupervised learning discovers abnormalities based on a precise characterization of expected behavior.				
Sarker et al. (2020)		Semi-supervised learning mixes supervised and unsupervised. RL, another ML topic.	Effective ML models require feature engineering and finding essential features. Cybersecurity data is complex and noisy, making it difficult to find meaningful information.		The two most common types of supervised learning techniques in the field of ML are classification and regression.	In unsupervised learning, data-driven techniques are used to find patterns, structures, or knowledge in unlabeled data.	DL's major benefit over traditional ML is improved performance on large amounts of security data.	RL, or environment-driven ML, lets an agent construct its own learning experiences by interacting with the world.		
										This study evaluates a new cybersecurity paradigm that considers established and developing ICT service standards.
										The study presented a generalized multi-layered ML-based cybersecurity data science model with data from several sources and analytics that support the latest data-driven patterns for intelligent security services.

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps of unsupervised	Benefits and limits of DL	RL to improve security	Future directions	Key findings
M. R. et al. (2021)		There are three categories of machine learning algorithms: supervised, and semi-supervised techniques.			When it comes to security, supervised learning algorithms can't see zero-day vulnerabilities.	Unsupervised learning systems can detect new assaults, but they produce too many false positives.				ML is increasingly used to construct anomaly detectors for mission-critical applications like Industrial Control Systems.
Abdelkhalak & Mashaly (2023)	ML can detect new day-zero attacks without knowing their network traffic signature.	In cybersecurity datasets, sample numbers for normal and risky conduct are often skewed.	It helps calculate several evaluations of the model's efficacy using specific terminology. The confusion matrix terms				DL can currently achieve great accuracy, surpassing standard ML models.			These findings support NIDS and improving marginalized population identification in data sets with high majority class detection.
Disha and Waheed (2022)		ML model reliability requires feature engineering and selection. However, cybersecurity data is complex and noisy, making it hard to spot critical pieces.	Accuracy, False Positive Rate, Precision, Recall, and other measures are used to evaluate ML-based IDS.	A supervised machine learning model predicts a discrete value as "attack" or "normal" in binary classification.				Incorporating reinforcement learning algorithms into the design of intelligent, self-improving cybersecurity systems.		
Ahmad et al. (2021)	The types of ML techniques used in cybersecurity include supervised, semi-supervised, and unsupervised learning.	There are four outcomes, and the Confusion Matrix counts them. It helps evaluate the model in several areas.		Supervised learning faces inequality. Unequal class distribution in the dataset is "imbalance." Skewed classifications originate from information gaps.						
Ortega-Fernandez et al. (2023)	ML techniques and applications help cybersecurity specialists improve their defences, detect assaults, and respond to developing cyber threats.	When labels are scarce, the method works well in supervised training but is difficult to apply in real life.	Cybersecurity anomaly detection often makes use of unsupervised learning techniques like Autoencoders.	DL models sensor dynamics and functional linkages to detect abnormalities using rule-based ML techniques.						The Deep Autoencoder model outperforms the state-of-the-art and baseline models in harder DDoS attacks.

Table 4.1. Cont.

Reference	Identification of Gaps	Applications of ML	Challenges & Limits of ML	Metrics methodologies	Vulnerabilities of Supervise Learning	Apps of unsupervised	Benefits and limits of DL	RL to improve security	Future directions	Key findings
Hnamte et al., (2023)		Traditional ML methods struggle to detect attacks with highly integrated features.					Recent improvements to IDS can be attributed to DL algorithm implementations.			This study presents an effective, efficient two-stage IDS for network behavior detection.
Kandhro et al. (2023)	The aforementioned identified topics present significant challenges in the current global context.	Both network and physical ICT security are improved by ML approaches.	A high false positive rate is the biggest issue with ML-based solutions.	This study investigates categorization performance criteria like accuracy, precision, FPR, FPR, and ROC.		The lack of sufficient training samples should be revealed by unsupervised learning methods.	Deep learning algorithms sometimes overfit, especially with limited or noisy training data.			
Vinayakumar et al. (2019)	Most datasets are scarce due to security and privacy considerations. dataset problems persist.					Unsupervised learning methods have improved cybersecurity by detecting anomalies.	Training DL models can be a time-consuming process that necessitates substantial computational resources.		Performance evaluation Upgraded hardware and distributed DNN training can improve IDS ML.	The study used the DNN model to detect attacks and intrusions using real-time host and network information.
Park et al. (2023)			Model overfitting and an inability to adapt to environmental changes like assault type render ML techniques unjustifiable.		ML-based intrusion detection classifiers are trained using supervised learning methods like the Random Forest algorithm.		Research has shown that deep learning systems are susceptible to environmental changes.		A multi-technology strategy, not just statistical analysis or ML/DL, is needed to overcome IDS limits.	Their ML-based attack-type classifier outperforms all other digital forensics tools for in-vehicle network attacks.
Pu et al. (2021)		ML algorithms for cyber IDS to boost detection rate and reduce false positives.			SVMs are a type of supervised learning model used to detect patterns in data.	IDSs prefer unsupervised ML to identify known and unknown assaults, including zero-day attacks.				The study's main finding shows that unsupervised ML works well in intrusion detection systems.
Siddiqi and Pak (2022)		NIDS secures networks. Everyone agrees that ML and DL-based NIDS best defends against complex network threats.	ML-based NIDSs may prevent network attacks. ML-based NIDS is hard to update for new network assaults.	Multiple criteria have been used to evaluate ML attack detection						Deep learning algorithms are known for their ability to understand network patterns, both normal and aberrant.

CHAPTER V

Discussion

This section presents a comprehensive analysis of the key findings obtained from the systematic literature review (SLR) on the evaluation of machine learning techniques in the domain of cybersecurity, along with their respective implications.

The continuous difficulty lies in the reliance on old datasets (De Carvalho Bertoli et al., 2021). There is a potential limitation in the accuracy of these datasets in capturing current cyber threats which gives rise to questions over the applicability of some of the research findings. To effectively tackle this matter, it is imperative to engage in continuous endeavors aimed at generating and preserving contemporary datasets that accurately depict the prevailing threat environments. According to Shaukat et al., (2020), there is a growing need for novel automated security approaches in response to the increasing security challenges that are emerging. Automated machine learning has the potential to effectively identify dynamic cyber threats. Future research should prioritize the development of machine learning models that possess adaptability and the ability to learn in real-time, enabling them to effectively respond and adapt to emerging threats. The need for efficient and automated cyber threat detection cannot be overstated, particularly in real-time situations (Seo et al., 2021). The prompt emphasizes the crucial nature of promptly detecting attacks to ensure the efficacy of cybersecurity measures. The primary focus of research endeavors should be directed toward the advancement of machine learning-based detection systems that effectively strike a compromise between expeditiousness and precision. The attainment of real-time threat identification necessitates the use of machine learning models that surpass existing methodologies (Kim and Pak, 2021). In addition, it is crucial to take into account system load factors. Machine learning models should demonstrate efficient performance while avoiding the imposition of unreasonable hardware demands. The researchers Latif et al., (2022) advocate the incorporation of real-time and streaming data analytics into the process of performance evaluation. The combination of several components promotes organizational agility and ensures the continued relevance of cybersecurity evaluation approaches. The primary emphasis of research should be directed towards the investigation of solutions that facilitate the seamless integration of data. According to Yong and Gao, (2023), the use of ensemble

learning approaches has the potential to improve the overall performance of cybersecurity systems. The evaluation of measures that effectively strike a balance between detection accuracy and false positives is of greatest significance. Further research should investigate the most effective combinations of models and ensemble procedures to optimize their performance. The integration of explainable artificial intelligence (AI) methods within the field of cybersecurity has the potential to improve transparency and comprehensibility, as highlighted by Koay et al. (2023). The integration of transparent machine learning (ML)-driven security systems has the potential to enhance collaborative efforts between human analysts and artificial intelligence (AI) tools. The utilization of deep learning architectures, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), exhibits the potential to enhance the process of identifying vulnerabilities in cybersecurity. These architectural designs provide improved levels of precision and effectiveness, hence justifying the need for additional investigation into their integration. The dual nature of machine learning in the field of cybersecurity, which encompasses both the augmentation of decision-making processes and the introduction of vulnerabilities, is a crucial aspect that requires careful examination (Ferreira et al., 2023). The utilization of machine learning in the context of security necessitates an intelligent strategy that takes into account both its benefits and the possible risks of misuse. To thoroughly evaluate the performance of a model, it is recommended to utilize complete evaluation criteria that go beyond accuracy, as suggested by Koay et al. (2023). When evaluating the practicality of a solution in real-world scenarios, it is imperative to take into account factors such as scalability, processing costs, and reliability. According to Leevy et al. (2021), the utilization of ensemble learning techniques has the potential to improve the effectiveness and dependability of cybersecurity systems. Further investigation is warranted to explore the most effective combinations of models and ensemble approaches in the context of threat detection.

Along with this, machine learning plays an essential role in enhancing cybersecurity measures. The technology provides the capacity to efficiently evaluate large volumes of data, identify irregularities, and adjust to changing security risks. Machine learning approaches, including supervised, unsupervised, and reinforcement learning, are extensively employed in the domains of intrusion detection, malware classification, and threat prediction. According to Zhang et al., (2022), the application

of deep learning techniques has resulted in enhanced precision of these models when it comes to detecting intricate cyber threats. Supervised learning methodologies have been widely employed in the field of cybersecurity, namely in the domains of classification and regression tasks. These technologies facilitate the identification of malicious software, the recognition of cyber threats, and the anticipation of diverse security concerns. Nevertheless, the utilization of big, labeled datasets poses a constraint due to the inherent difficulty in acquiring and sustaining them (Prazeres et al., 2023). Unsupervised learning methods, specifically clustering algorithms, have been employed to detect patterns and anomalies in network traffic and user behavior. These entities demonstrate exceptional proficiency in identifying concealed risks and possess the capability to analyse unannotated data, rendering them highly advantageous in the context of instantaneous hazard identification. However, the performance of clustering algorithms is contingent upon the quality of the data and the selection of an appropriate algorithm, (WISAnwanichthan and Thammawichai, 2021). The utilization of deep learning methods in the field of cybersecurity has been prominent as a result of their capacity to autonomously extract characteristics from complex and multi-dimensional datasets. These technologies find application in a wide range of contexts, including intrusion detection and malware classification. Deep learning models, such as convolutional and recurrent neural networks, have exhibited exceptional performance. Nevertheless, the acquisition and management of significant volumes of data and computing resources offer considerable challenges, (Liu et al., 2021). The application of reinforcement learning in the field of cybersecurity, namely in the domain of intrusion detection, has exhibited considerable potential. Reinforcement learning (RL) agents demonstrate the capability to effectively respond to dynamic threats through the utilization of past data and real-time interactions with the environment, hence enabling them to adapt accordingly. According to (Bland et al., 2020), security systems are improved in terms of accuracy and efficiency through the utilization of these technologies. Moreover, they demonstrate particular proficiency in managing sophisticated and ever-changing threats. The evaluation of machine learning techniques in the realm of cybersecurity is now seeing notable transformations. The utilization of adversarial machine learning techniques is employed to evaluate the efficacy of model defenses against highly advanced threats. The integration of real-time data analysis capabilities into evaluation processes is being undertaken to effectively address growing risk factors. The utilization of

hardware accelerators, such as field-programmable gate arrays (FPGAs), has also been observed in the enhancement of cyberattack detection, Latif et al. (2022) and Shaukat et al. (2020).

CHAPTER VI

Conclusion and Future work

The field of cybersecurity is characterized by constant change, as adversaries consistently develop and broaden their strategies. Machine learning has emerged as a viable solution, presenting a potentially effective set of tools to address these dynamic challenges. This systematic literature analysis was conducted to comprehensively evaluate the efficacy of machine learning approaches in the field of cybersecurity. Through this process, we have gained valuable insights and identified significant problems that will influence future advancements in this area.

The Issue of Obsolete Datasets and the Challenge of Relevance: A significant challenge that emerged from our analysis was the utilization of outdated datasets in the realm of cybersecurity research. The datasets DARPA 1998, KDD-CUP '99, and NSL-KDD among others have played a significant role in the past; nonetheless, their current relevance has raised questions. The dynamic nature of the threat landscape requires datasets that accurately reflect the present state of challenges and vulnerabilities. The focus of research endeavors should be directed at the collection and dissemination of datasets that effectively cover the current landscape of cyber risks.

The Automation Imperative for Emerging Risks: It is widely agreed upon by security professionals that the use of new and automated security solutions is crucial in effectively mitigating rising threats. The rapid emergence of new risks necessitates the development of adaptive systems that possess the ability to promptly identify and respond to these threats. The branch of machine learning, specifically automated machine learning (AutoML), is becoming recognized as a helpful tool in this context. AutoML simplifies the process of selecting models, setting hyperparameters, and engineering features, hence facilitating the deployment of efficient cybersecurity solutions that address dynamic threats for enterprises.

Enhancing Real-Time Cyber Threat Detection Efficiency: Efficiency in the detection of cyber threats is an additional significant challenge. In the contemporary digital environment, the speed at which actions are executed can significantly determine the outcome, ranging from a minor security breach to a catastrophic cyberattack. The ability to detect and respond to attacks in real-time is crucial for

promptly recognizing and limiting their impact. Furthermore, it is imperative to construct machine learning models with a focus on efficiency, ensuring that they can function without imposing unreasonable hardware demands, especially in situations with limited resources.

The incorporation of real-time data analytics: The incorporation of real-time and streaming data analytics has arisen as a significant factor to be taken into account. For technology to effectively address the dynamic nature of the threat landscape, cybersecurity solutions must exhibit a high degree of adaptability and responsiveness. The utilization of real-time data analytics not only facilitates the rapid identification of threats but also provides significant insights into ongoing attacks. The incorporation of real-time capabilities into evaluation procedures is of the greatest significance when seeking to effectively respond to the dynamic and ever-changing cybersecurity landscape.

The utilization of ensemble learning techniques in the context of explainable artificial intelligence (AI) is a topic of interest: Ensemble learning approaches have emerged as a powerful approach to enhance the overall performance of cybersecurity systems. The balance between the precision of detection and the occurrence of false positives, along with the practical consequences of false alarms, highlights the significance of evaluating metrics that take into account both of these factors. In addition, the utilization of explainable AI techniques plays a crucial role in enhancing the levels of transparency and comprehensibility inside ML-driven security systems. The establishment of transparent and comprehensible decision-making procedures is crucial in building trust in cybersecurity solutions.

The study explores deep learning architectures and their applications in both positive and negative contexts: Deep learning architectures, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), exhibit the potential to improve the detection of cybersecurity vulnerabilities. Their ability to efficiently process complex and high-dimensional datasets can enhance both accuracy and efficiency in detecting threats. Nevertheless, it is essential to maintain a sense of the inherent duality of machine learning in the realm of cybersecurity. While the utilization of this technology improves the overall performance of systems and aids in

the process of decision-making, it is important to acknowledge that it can also be vulnerable to manipulation by those with evil intent, who may employ advanced techniques to carry out attacks. The existence of this contradiction highlights the necessity for thorough and meticulous research as well as thorough implementation.

Evaluation Metrics and Ensemble Learning: A Comprehensive Review in this thesis, we present an updated evaluation of metrics and ensemble learning techniques. We aim to provide a comprehensive review of the current state of research in this field. Our analysis focuses on the latest advancements and methodologies used in evaluating the performance of ML techniques in the context of cybersecurity. Moreover, we propose the utilization of evaluation criteria beyond accuracy to conduct a full assessment of model performance. Scalability, temporal and computational expenses, and dependability are crucial factors to guarantee practical viability in real-world scenarios. Ensemble learning techniques provide a mechanism for integrating several models, hence improving the efficiency and dependability of cybersecurity systems.

In summary, the progress of machine learning in the field of cybersecurity relies on the resolution of these gaps and limitations to enable to protection of the efficacy and flexibility of ML methodologies in preventing ever-changing cyber threats. The continuous development of the digital domain necessitates a commensurate advancement in our level of readiness. By incorporating the perspectives and advancements highlighted in this thorough review, we may strengthen our defensive capabilities and maintain a competitive advantage in the continuously intensifying cyber warfare.

6.1 Future Directions

The findings indicate potential avenues for future research and development in the domain of machine learning and cybersecurity, which are outlined below:

- **Dataset Modernization:** The objective is to create and sustain datasets that are current and accurately represent prevailing cyber risks.
- **Advancements in Automation:** Emphasizing the automation of security systems to effectively respond to evolving and emerging threats.
- **Enhancing Efficiency:** Place emphasis on the advancement of machine learning models that are effective in real-time threat detection while minimizing hardware resource demands.

- **Real-time Integration:** Explore strategies for seamlessly integrating real-time data analytics into ML-driven security systems.
- **Deep Learning Integration:** Look at how deep learning architectures can be integrated to enhance threat detection.
- **Holistic Evaluation:** Establish consistent evaluation frameworks that take scalability, processing costs, and reliability into account.
- **Ensemble Learning:** Examine the best model combinations and ensemble methods for enhancing the performance of cybersecurity systems.
- **Interdisciplinary cooperation:** Building more reliable models and methods requires cooperation between machine learning researchers and cybersecurity specialists. The utilization of an interdisciplinary approach has the potential to yield novel solutions that effectively tackle the ever-changing landscape of cyber threats.
- **Adversarial Defense:** Future research should concentrate on strengthening model robustness and creating safeguards against adversarial manipulation, given that machine learning models are susceptible to adversarial attacks.
- **Hardware Optimization:** The performance of cyberattack detection systems can be greatly enhanced by future developments in hardware acceleration, such as FPGAs. Research should focus on developing specialized hardware for machine learning in cybersecurity.
- **Ethical Issues:** As machine learning models are increasingly incorporated into cybersecurity procedures, ethical issues relating to data privacy, bias, and transparency must be thoroughly addressed.

In conclusion, it is essential to recognize the importance of resolving the identified gaps and limits to further enhance the implementation of machine learning in the realm of cybersecurity. In anticipation of future developments, there is an emerging demand for a heightened focus on standardized evaluation methodologies, the integration of empirical data from real-world contexts into evaluations, and the reinforcement of model strength against adversarial attacks. To optimize the utilization of machine learning in the field of cybersecurity, it is imperative to implement methodologies that address the challenges related to imbalanced data and provide the reliable interpretability of models.

Machine learning is a highly effective technology in the realm of cybersecurity since it provides improved efficacy in the detection and mitigation of

cyber threats. Nevertheless, it is imperative to acknowledge the inherent difficulties associated with data accessibility, vulnerabilities in models, and the capacity to conduct real-time analysis. Future research efforts should be focused on tackling these issues and advancing the area, finally ensuring the implementation of protocols for cybersecurity that are flexible and adaptable.

6.2 Recommendation

Future research and activities in the field of machine learning in cybersecurity are encouraged to take into account the following based on the findings of this SLR and the highlighted gaps and issues in the field.

- The collection and utilization of current datasets that faithfully represent modern cyber risks should be prioritized by researchers, practitioners, and organizations involved in cybersecurity. Training machine learning models to detect and prevent changing threats requires datasets to be regularly updated.
- The cybersecurity industry should put money into researching and implementing cutting-edge automated security solutions. Particularly in real-time circumstances, these approaches need to prioritize fast and accurate threat detection. Organizations can respond more quickly and efficiently to new cyber threats if they use automation to help them stay one step ahead of their opponents.
- There is a growing requirement for transparency and explainability as machine learning models become increasingly important to cybersecurity operations. Adopting interpretable AI strategies can make model decisions more easily understood, leading to more trust and better, more well-informed choices.
- More research into the potential benefits of incorporating ensemble learning approaches into cybersecurity systems is warranted. The use of ensemble approaches can increase the accuracy and reliability of threat detection by combining the capabilities of numerous models.
- Cybersecurity strategies should take into account the use of real-time and streaming data analytics. Security measures can be kept in step with the ever-changing cyber threat landscape by employing this method of proactive threat detection and response.
- Designing ML-driven cybersecurity solutions with efficiency and minimal resource requirements in mind is essential. Models should be able to function well without requiring excessive hardware, making mass adoption possible.

- In addition to accuracy, other criteria such as scalability, time and processing costs, and reliability should be used to evaluate machine learning models for cybersecurity. Insight into a model's practicality and performance in the actual world is enhanced by these measurements.
- Sharing of information and expertise is essential in the field of cybersecurity, hence cooperation between academics, industry professionals, and government agencies is essential. Sharing information, creating universal standards for review, and establishing best practices can all help move the needle faster.

The field of ML and cybersecurity can improve its defenses against the wide variety of cyber threats by implementing these suggestions. By taking these measures, we can improve the security of our most precious digital assets and infrastructure through the use of machine learning.

Reference

- Abdelkhalek, A., & Mashaly, M. (2023). Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning. *The Journal of Supercomputing*, 79(10), 10611–10644. <https://doi.org/10.1007/s11227-023-05073-x>
- Agnew, D., Aljohani, N., Mathieu, R., Boamah, S., Nagaraj, K., McNair, J., & Bretas, A. (2022). Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation. *Applied Sciences*, 12(14), 6868. <https://doi.org/10.3390/app12146868>
- Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2023). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & Security*, 124, 102959. <https://doi.org/10.1016/j.cose.2022.102959>
- Ahmad, M., Riaz, Q., Zeeshan, M., Tahir, H., Haider, S. A., & Khan, M. S. (2021). Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. *EURASIP Journal on Wireless Communications and Networking*, 2021(1), 10. <https://doi.org/10.1186/s13638-021-01893-8>
- Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, 2(3), 527–555. <https://doi.org/10.3390/jcp2030027>
- Aljabri, M., & Mohammad, R. M. A. (2023). Click fraud detection for online advertising using machine learning. *Egyptian Informatics Journal*, 24(2), 341–350. <https://doi.org/10.1016/j.eij.2023.05.006>
- Almashhadani, A. O., Kaiiali, M., Carlin, D., & Sezer, S. (2020). MaldomDetector: A system for detecting algorithmically generated domain names with machine learning. *Computers & Security*, 93, 101787. <https://doi.org/10.1016/j.cose.2020.101787>

- Aloraini, F., Javed, A., Rana, O., & Burnap, P. (2022). Adversarial machine learning in IoT from an insider point of view. *Journal of Information Security and Applications*, 70, 103341. <https://doi.org/10.1016/j.jISA.2022.103341>
- Alshammari, F. H. (2023). Design of capability maturity model integration with cybersecurity risk severity complex prediction using bayesian-based machine learning models. *Service Oriented Computing and Applications*, 17(1), 59–72. <https://doi.org/10.1007/s11761-022-00354-4>
- Al-Taleb, N., & Saqib, N. (2022). Towards a Hybrid Machine Learning Model for Intelligent Cyber Threat Identification in Smart City Environments. *Applied Sciences*, 12(4), 1863. <https://doi.org/10.3390/app12041863>
- Apruzzese, G., Andreolini, M., Marchetti, M., Venturi, A., & Colajanni, M. (2020). Deep Reinforcement Adversarial Learning Against Botnet Evasion Attacks. *IEEE Transactions on Network and Service Management*, 17(4), 1975–1987. <https://doi.org/10.1109/TNSM.2020.3031843>
- Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023a). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, 4(1), 1–38. <https://doi.org/10.1145/3545574>
- Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). A Machine Learning Security Framework for Iot Systems. *IEEE Access*, 8, 114066–114077. <https://doi.org/10.1109/ACCESS.2020.2996214>
- Bari, B. S., Yelamarthi, K., & Ghafoor, S. (2023). Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study. *Sensors*, 23(7), 3610. <https://doi.org/10.3390/s23073610>
- Basheer, L., & Ranjana, P. (2022). A Comparative Study of Various Intrusion Detections In Smart Cities Using Machine Learning. *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, 1–6. <https://doi.org/10.1109/ICIBT52874.2022.9807724>

- Berghout, T., Benbouzid, M., & Muyeen, S. M. (2022). Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *International Journal of Critical Infrastructure Protection*, 38, 100547. <https://doi.org/10.1016/j.ijcip.2022.100547>
- Bitirgen, K., & Filik, Ü. B. (2023). A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. *International Journal of Critical Infrastructure Protection*, 40, 100582. <https://doi.org/10.1016/j.ijcip.2022.100582>
- Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine Learning Cyberattack and Defense Strategies. *Computers & Security*, 92, 101738. <https://doi.org/10.1016/j.cose.2020.101738>
- Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabé, J. B., Baldini, G., & Skarmeta, A. (2022). Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks*, 203, 108661. <https://doi.org/10.1016/j.comnet.2021.108661>
- Chakir, O., Rehaimi, A., Sadqi, Y., Abdellaoui Alaoui, E. A., Krichen, M., Gaba, G. S., & Gurtov, A. (2023). An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0. *Journal of King Saud University - Computer and Information Sciences*, 35(3), 103–119. Scopus. <https://doi.org/10.1016/j.jksuci.2023.02.009>
- De Carvalho Bertoli, G., Pereira Junior, L. A., Saotome, O., Dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., Barbieri, S., Rodrigues, M. S., & Parente De Oliveira, J. M. (2021). An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System. *IEEE Access*, 9, 106790–106805. Scopus. <https://doi.org/10.1109/ACCESS.2021.3101188>
- Disha, R. A., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest

- (GIWRF) feature selection technique. *Cybersecurity*, 5(1), 1. <https://doi.org/10.1186/s42400-021-00103-8>
- Ezugwu, A. E., Oyelade, O. N., Ikotun, A. M., Agushaka, J. O., & Ho, Y.-S. (2023). Machine Learning Research Trends in Africa: A 30 Years Overview with Bibliometric Analysis Review. *Archives of Computational Methods in Engineering*. <https://doi.org/10.1007/s11831-023-09930-z>
- Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*, 124, 102954. <https://doi.org/10.1016/j.cose.2022.102954>
- Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. <https://doi.org/10.1016/j.jISA.2019.102419>
- Ferreira, L., Silva, D. C., & Itzazelaia, M. U. (2023). Recommender Systems in Cybersecurity. *Knowledge and Information Systems*. <https://doi.org/10.1007/s10115-023-01906-6>
- Hnamte, V., Nhung-Nguyen, H., Hussain, J., & Hwa-Kim, Y. (2023). A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE. *IEEE Access*, 11, 37131–37148. <https://doi.org/10.1109/ACCESS.2023.3266979>
- Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T.-H. (2022). Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey. *IEEE Access*, 10, 121173–121192. <https://doi.org/10.1109/ACCESS.2022.3220622>
- Kandhro, I. A., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures. *IEEE Access*, 11, 9136–9148. <https://doi.org/10.1109/ACCESS.2023.3238664>
- Kattamuri, S. J., Penmatsa, R. K. V., Chakravarty, S., & Madabathula, V. S. P. (2023). Swarm Optimization and Machine Learning Applied to PE Malware Detection towards Cyber

- Threat Intelligence. *Electronics*, 12(2), 342.
<https://doi.org/10.3390/electronics12020342>
- KhraISat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1), 20.
<https://doi.org/10.1186/s42400-019-0038-7>
- Kim, T., & Pak, W. (2021). Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System. *IEEE Access*, 9, 83806–83817.
<https://doi.org/10.1109/ACCESS.2021.3087201>
- Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, 60(2), 377–405. <https://doi.org/10.1007/s10844-022-00753-1>
- Kosmanos, D., Pappas, A., Maglaras, L., Moschoyiannis, S., Aparicio-Navarro, F. J., Argyriou, A., & Janicke, H. (2020). A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles. *Array*, 5, 100013.
<https://doi.org/10.1016/j.array.2019.100013>
- Latif, S., Huma, Z. E., Jamal, S. S., Ahmed, F., Ahmad, J., Zahid, A., Dashtipour, K., Aftab, M. U., Ahmad, M., & Abbasi, Q. H. (2022). Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network. *IEEE Transactions on Industrial Informatics*, 18(9), 6435–6444. <https://doi.org/10.1109/TII.2021.3130248>
- Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. *IEEE Access*, 7, 165607–165626.
<https://doi.org/10.1109/ACCESS.2019.2953095>
- Leevy, J. L., Hancock, J., Zuech, R., & Khoshgoftaar, T. M. (2021). Detecting cybersecurity attacks across different network features and learners. *Journal of Big Data*, 8(1), 38.
<https://doi.org/10.1186/s40537-021-00426-w>

- Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. *IEEE Access*, 7, 158126–158147. <https://doi.org/10.1109/ACCESS.2019.2948912>
- Liu, Q., Li, Z., Yuan, S., Zhu, Y., & Li, X. (2021). Review on Vehicle Detection Technology for Unmanned Ground Vehicles. *Sensors*, 21(4), 1354. <https://doi.org/10.3390/s21041354>
- M. R., G. R., Ahmed, C. M., & Mathur, A. (2021). Machine learning for intrusion detection in industrial control systems: Challenges and lessons from experimental evaluation. *Cybersecurity*, 4(1), 27. <https://doi.org/10.1186/s42400-021-00095-5>
- Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, 10(10), 2823–2836. <https://doi.org/10.1007/s13042-018-00906-1>
- Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet*, 15(2), 83. <https://doi.org/10.3390/fi15020083>
- Ortega-Fernandez, I., Sestelo, M., Burguillo, J. C., & Piñón-Blanco, C. (2023). Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. *Wireless Networks*. <https://doi.org/10.1007/s11276-022-03214-3>
- Ortiz, E. C., & Reinerman-Jones, L. (2015). Theoretical Foundations for Developing Cybersecurity Training. In R. Shumaker & S. Lackey (Eds.), *Virtual, Augmented and Mixed Reality* (Vol. 9179, pp. 480–487). Springer International Publishing. https://doi.org/10.1007/978-3-319-21067-4_49
- Park, S. B., Jo, H. J., & Lee, D. H. (2023). G-IDCS: Graph-Based Intrusion Detection and Classification System for CAN Protocol. *IEEE Access*, 11, 39213–39227. <https://doi.org/10.1109/ACCESS.2023.3268519>

- Prazeres, N., Costa, R. L. D. C., Santos, L., & Rabadão, C. (2023). Engineering the application of machine learning in an IDS based on IoT traffic flow. *Intelligent Systems with Applications*, 17, 200189. <https://doi.org/10.1016/j.iswa.2023.200189>
- Pu, G., Wang, L., Shen, J., & Dong, F. (2021). A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Science and Technology*, 26(2), 146–153. <https://doi.org/10.26599/TST.2019.9010051>
- Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques. *International Journal of Environmental Research and Public Health*, 17(24), 9347. <https://doi.org/10.3390/ijerph17249347>
- Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., & Bolla, R. (2021). An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains. *Journal of Network and Systems Management*, 29(4), 37. <https://doi.org/10.1007/s10922-021-09607-7>
- Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability (Switzerland)*, 14(18). Scopus. <https://doi.org/10.3390/su141811213>
- Sarker, I. H. (2022). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*. <https://doi.org/10.1007/s40745-022-00444-2>
- Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7(1), 41. <https://doi.org/10.1186/s40537-020-00318-5>
- Seo, S., Han, S., Park, J., Shim, S., Ryu, H.-E., Cho, B., & Lee, S. (2021). Hunt for Unseen Intrusion: Multi-Head Self-Attention Neural Detector. *IEEE Access*, 9, 129635–129647. Scopus. <https://doi.org/10.1109/ACCESS.2021.3113124>

- Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020a). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, 8, 222310–222354. <https://doi.org/10.1109/ACCESS.2020.3041951>
- Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., Chen, S., Liu, D., & Li, J. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*, 13(10), 2509. <https://doi.org/10.3390/en13102509>
- Siddiqi, M. A., & Pak, W. (2022). Tier-Based Optimization for Synthesized Network Intrusion Detection System. *IEEE Access*, 10, 108530–108544. <https://doi.org/10.1109/ACCESS.2022.3213937>
- Talukder, Md. A., Hasan, K. F., Islam, Md. M., Uddin, Md. A., Akhter, A., Yousuf, M. A., Alharbi, F., & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. *Journal of Information Security and Applications*, 72, 103405. <https://doi.org/10.1016/j.jISA.2022.103405>
- Tanner, E. M., Bornehag, C.-G., & Gennings, C. (2019). Repeated holdout validation for weighted quantile sum regression. *MethodsX*, 6, 2855–2860. <https://doi.org/10.1016/j.mex.2019.11.008>
- The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. (2023). *Iraqi Journal for Computer Science and Mathematics*, 87–101. <https://doi.org/10.52866/ijcsm.2023.01.01.008>
- Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, 7, 41525–41550. <https://doi.org/10.1109/ACCESS.2019.2895334>
- Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, 8(3), 313–321. <https://doi.org/10.1016/j.icte.2022.04.007>

- WISAnwanichthan, T., & Thammawichai, M. (2021). A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM. *IEEE Access*, *9*, 138432–138450. <https://doi.org/10.1109/ACCESS.2021.3118573>
- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, *6*, 35365–35381. <https://doi.org/10.1109/ACCESS.2018.2836950>
- Yong, X., & Gao, Y. (2023). Hybrid Firefly and Black Hole Algorithm Designed for XGBoost Tuning Problem: An Application for Intrusion Detection. *IEEE Access*, *11*, 28551–28564. Scopus. <https://doi.org/10.1109/ACCESS.2023.3259981>
- Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, *10*, 93104–93139. <https://doi.org/10.1109/ACCESS.2022.3204051>

Appendices

Appendix A:

Ethical Committee Approval Letter



NEAR EAST UNIVERSITY

SCIENTIFIC RESEARCH ETHICS COMMITTEE

24.10.2023

Dear Adam Muhammad

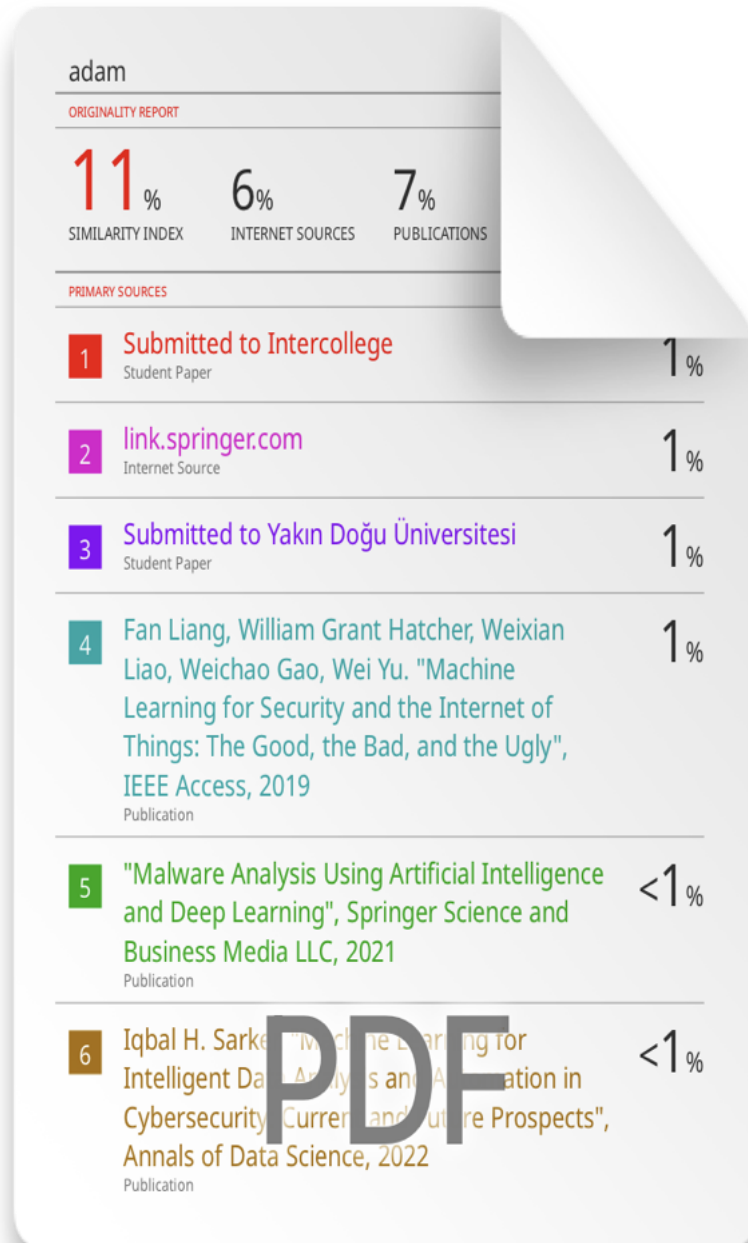
Your project **“A Systematic Literature Review: Performance Evaluation Of Machine Learning Techniques In Cybersecurity”** has been evaluated. Since only secondary data will be used the project does not need to go through the ethics committee. You can start your research on the condition that you will use only secondary data.

Prof. Dr. Aşkın KIRAZ

The Coordinator of the Scientific Research Ethics Committee

Appendix B: Turnitin Similarity Report





- | | | |
|----|---|-----|
| 7 | www.ijraset.com
Internet Source | |
| 8 | ebin.pub
Internet Source | |
| 9 | Mohammad Wazid, Ashok Kumar D, Chamola, Youngho Park. "Uniting cy security and machine learning: Advantages, challenges and future research", ICT Express, 2022
Publication | |
| 10 | Zhibo Zhang, Hussam Al Hamadi, Ernesto Damiani, Chan Yeob Yeun, Fatma Taher. "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research", IEEE Access, 2022
Publication | <1% |
| 11 | journalofbigdata.springeropen.com
Internet Source | <1% |
| 12 | Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli et al. "The Role of Machine Learning in Cybersecurity", Digital Threats: Research and Practice, 2022
Publication | <1% |
| 13 | Kun Sun, Jiaying an. Model of Storm Surge Maximum Water Level Increases in a Coastal Area Using Ensemble machine Learning and | <1% |

PDF

Explicable Algorithm", Earth and Space Science, 2023

Publication

- 14 Abigail M. Y. Koay, Ryan K. L. Ko, Hironori Hattema, Kenneth Radke. "Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges", Journal of Intelligent Information Systems, 2022

Publication

- 15 www.researchgate.net <1%

Internet Source

- 16 www.mdpi.com <1%

Internet Source

- 17 ijritcc.org <1%

Internet Source

- 18 "Advances in Information, Communication and Cybersecurity", Springer Science and Business Media LLC, 2022 <1%

Publication

- 19 Rayeesa Malik, Yashwant Singh, Zakir Ahmad Sheikh, Pooja Anand, Pradeep Kumar Singh, Tewabe Chekele Workneh. "An Improved Deep Belief Network (DBN) on Topology Based Network for Traffic Systems", Journal of Advanced Transportation, 2022 <1%

Publication

PDF

- 20 Submitted to Asia Pacific University
Technology and Innovation (UCTI)
Student Paper
-
- 21 Jonghoon Lee, Jonghyun Kim, Ikkyu
Kijun Han. "Cyber Threat Detection
Artificial Neural Networks using Eve
Profiles", IEEE Access, 2019
Publication
-
- 22 Submitted to CSU, San Jose State University <1%
Student Paper
-
- 23 Gustavo De Carvalho Bertoli, Lourenco Alves
Pereira, Osamu Saotome, Aldri L. Santos et al. <1%
"An end-to-end framework for machine
learning-based network intrusion detection
system", IEEE Access, 2021
Publication
-
- 24 Zubaida Rehman, Noshina Tariq, Syed Atif
Moqurrab, Joon Yoo, Gautam Srivastava. <1%
"Machine learning and internet of things
applications in enterprise architectures:
Solutions, challenges, and open issues",
Expert Systems, 2023
Publication
-
- 25 Radwan Qasbi, Faik Anwar, Stephanny
VicunaPolo, Dalia J. Al-Hadi et al. <1%
"Machine learning techniques for predicting
depression and anxiety in pregnant and

postpartum women during the COVID-19 pandemic: a cross-sectional regional study. *Journal of Clinical Pharmacy and Therapeutics*, 2022

Publication

26 Submitted to Liverpool John Moores University

Student Paper

27 Sepp Hochreiter, Jürgen Schmidhuber. "Long Short-Term Memory", *Neural Computation*, 1997

Publication

<1%

28 Submitted to The Hong Kong Polytechnic University

Student Paper

<1%

29 Submitted to Hofstra University

Student Paper

<1%

30 dspace.unimap.edu.my

Internet Source

<1%

31 John Audu, Adeyemi Adegbenjo, Emmanuel Ajisegiri, Simone Irtwange. "Enhancing Yam Quality Detection through Computer Vision in IoT and Robotics Applications", *Research Square Platform LLC*, 2023

Publication

<1%

32 B. Rekha, S. R. S. Reddy, S. P. S. Sridharana, G. Kavya. "Chapter 45 The Prediction of Attacks and Challenges in Cyber Security Using

<1%

PDF

Biomechanics and Biomedical Engineering
Imaging & Visualization, 2023

Publication

- 41 Barshan Dev, Md Ashikur Rahman, Jahidul Islam, Md Zillur Rahman, De
"Properties prediction of composite
on machine learning models: A focus
statistical index approaches", Materials Today
Communications, 2024

Publication

- 42 worldwidescience.org <1%
Internet Source

- 43 Aryan Chopra, Aditya Modi, Brijendra Singh.
"chapter 2 Machine Learning Algorithm With
TensorFlow and SciKit for Next Generation
Systems", IGI Global, 2023 <1%

Publication

- 44 Johnson Adeleke Adeyiga, Philip Gbounmi
Toriola, Temitope Elizabeth Abioye(Ogunbiyi),
Adebisi Esther Oluwatosin et al. "Fake News
Detection Using a Logistic Regression Model
and Natural Language Processing
Techniques", Research Square Platform LLC,
2023 <1%

Publication

- 45 Submitted to University of Ibadan <1%
Student Paper

PDF