Cite this research:
Yaseen, A.,(2023). The Role of Machine Learning in Network Anomaly Detection for Cybersecurity SSRAML SageScience, 1(1), 1–15.

The Role of Machine Learning in Network Anomaly Detection for Cybersecurity

Asad Yaseen
Asad4ntrp2@gmail.com
https://orcid.org/0009-0002-8950-0767

check for updates

Article history:
Received:
April/12/2023
Accepted:
July/08/2023

Abstract

This research introduces a theoretical framework for network anomaly detection in cybersecurity, emphasizing the integration of adaptive machine learning models, ensemble techniques, and advanced feature engineering. The adaptability of machine learning models enables dynamic responsiveness to emerging cyber threats, forming a foundation for a resilient anomaly detection system. Ensemble techniques, particularly the incorporation of Random Forests, enhance the framework's robustness by amalgamating strengths from diverse models, mitigating false positives and negatives. Advanced feature engineering, coupled with deep learning architectures, contributes to a nuanced understanding of intricate patterns within network traffic. The theoretical exploration encounters challenges in quantifying performance gains, integration complexities, and data privacy concerns. Addressing these challenges is critical for refining and fortifying the proposed framework, ensuring its applicability and effectiveness in real-world cybersecurity scenarios. The significance of the framework lies in addressing existing gaps in network anomaly detection theories and advancing the understanding of machine learning's role in cybersecurity. Future directions include refining adaptive models, enhancing ensemble techniques, and addressing data privacy concerns. Adapting theoretical approaches to meet emerging cyber threats is paramount for the continual evolution of theoretical frameworks in cybersecurity. This research underscores the importance of ongoing theoretical advancements for practical applications, fostering optimism for the continual growth of frameworks that effectively combat the ever-changing landscape of cybersecurity challenges.

Keywords: Anomaly detection, Cybersecurity, Adaptive machine learning, Ensemble techniques, Feature engineering, Performance quantification, Integration complexities

Introduction

In the evolving landscape of cybersecurity, the significance of network anomaly detection has become paramount. As cyber threats grow in sophistication, traditional security mechanisms struggle to cope with the sheer variety and complexity of these threats. Network anomaly detection emerges as a crucial defensive strategy, designed to identify unusual patterns or behaviors in network traffic that could signify a potential security breach or cyberattack. This dissertation delves into the integration of machine learning (ML) in enhancing network anomaly detection, offering a theoretical exploration into this contemporary and vital field. The pertinence of network anomaly detection in cybersecurity cannot be overstated. With an increasing reliance on digital infrastructure, the consequences of security breaches have become more severe, impacting everything from individual privacy to national security. Traditional security measures, often rule-based and static, are proving inadequate in the face of adaptive and sophisticated cyber threats. This inadequacy has catalyzed the search for more dynamic and intelligent solutions, leading to the integration of machine learning techniques. Machine learning, with its ability to learn from data, adapt, and identify patterns, offers a promising avenue to revolutionize network anomaly detection. By leveraging ML, systems can potentially detect novel or evolving threats that elude traditional detection mechanisms. The purpose of this theoretical exploration is to comprehensively understand the role of machine learning in network anomaly detection within the

realm of cybersecurity. This dissertation aims to achieve several objectives: firstly, to provide a detailed overview of the current state of network anomaly detection and the challenges it faces; secondly, to explore how machine learning can address these challenges and enhance detection capabilities; and thirdly, to develop a theoretical framework that integrates ML into network anomaly detection in a meaningful and effective way. This framework will not only incorporate existing knowledge and practices but also seek to advance the field by proposing innovative approaches and methodologies. To accomplish these objectives, the dissertation begins with a thorough literature review, analyzing existing theoretical frameworks, models, and methodologies related to network anomaly detection and machine learning in cybersecurity. This review will highlight key concepts, identify gaps and evolving trends, and set the stage for the development of a new theoretical framework.

Following this, the research presents a comprehensive theoretical framework, underpinned by relevant assumptions and principles, and demonstrates how this framework aligns with and contributes to existing theories in the field. The practical application of this theoretical framework is then explored, discussing how it can be implemented in real-world scenarios and the potential benefits and implications of its application. A comparison with existing theories and models is conducted to contextualize the proposed framework within the broader landscape of network anomaly detection and machine learning in cybersecurity. The dissertation then delves into a discussion, interpreting the theoretical implications of the framework, addressing challenges and limitations, and exploring potential refinements and extensions. this dissertation aims to contribute significantly to the field of cybersecurity by providing a deeper theoretical understanding of the integration of machine learning in network anomaly detection. Through this exploration, it seeks to highlight the importance of ML in enhancing detection capabilities and advancing the field to better prepare for and respond to the ever-evolving landscape of cyber threats.

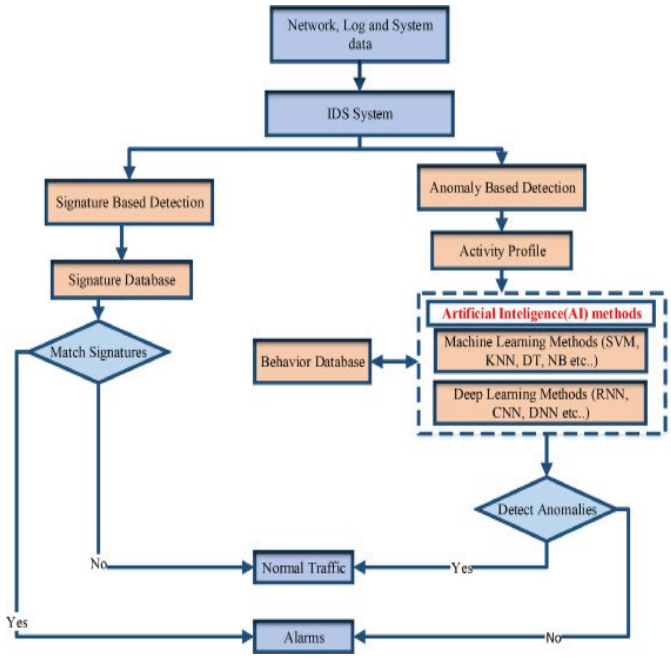

Figure 1: Machine Learning in Network Anomaly
(Source: https://ars.els-cdn.com/content/image/1-s2.0-S1389128621000141-gr4.jpg)

Literature Review

Empirical Study

Evaluating Machine Learning Approaches for Anomaly Detection and Addressing Key Challenges: According to Kayode-Ajala, 2021, In this study, two distinct datasets from industrial settings are analyzed to detect anomalies indicative of cyber attacks. The first dataset involves using Support Vector Machines (SVMs) to identify seven different attack categories and 35 subtypes. Despite the presence of considerable missing data, this method achieves promising results, with accuracy and F1-scores reaching up to 92.5% and 85.2%, respectively. The second dataset, named DS2, encompasses OPC UA-based traffic from a real-world Festo Didactic MPS PA Compact Workstation. Due to the limited occurrence of attacks (only two instances), a one-class SVM approach is adopted, resulting in an accuracy of 90.8%. However, the near-perfect recall rate leads to an impressive F1-score of 94.9% [1]. The research addresses crucial issues such as handling missing data and the selection of relevant features, which are common challenges in real-world datasets. These datasets often include noise and irrelevant information, necessitating effective feature selection strategies. Random Forest algorithms play a significant role in this context, enabling the calculation of the importance of individual features and the detection of anomalies. Moreover, techniques like Principal Component Analysis (PCA) are employed to reduce the feature space, focusing on the most pertinent features. Given the increasing frequency and severity of attacks on industrial environments, the efficacy of anomaly detection is paramount. Machine learning methods, particularly SVMs and Random Forests, demonstrate considerable potential in enhancing the detection capabilities of industrial Intrusion Detection Systems (IDSs) [1]. These approaches benefit from the limited variability in industrial settings and the abundant training data generated in such environments. The algorithms evaluated in this study successfully detect between 90% and 95% of attacks. However, this still leaves a small percentage of undetected attacks in industrial networks, posing ongoing security risks. Therefore, additional measures are necessary to further improve security levels in these critical environments.

Comprehensive Evaluation of Machine Learning Algorithms for Anomaly Detection: As per the Study Elmrabit et al., 2020, This research paper delves into the critical challenge of detecting malicious attacks in peer-to-peer smart grid platforms, focusing on the adaptability of attackers' behaviors. This evaluated twelve Machine Learning (ML) algorithms for their efficacy in identifying anomalous activities in network systems, utilizing three publicly available datasets: CICIDS-2017, UNSW-NB15, and the Industrial Control System (ICS) cyberattack datasets. The experimental analysis was conducted through the University of Leicester's ALICE high-performance computing facility, offering a thorough comparison of these ML techniques. This findings indicate that the Random Forest (RF) algorithm outperformed others across multiple evaluation metrics including accuracy, precision, recall, F1-Score, and Receiver Operating Characteristic (ROC) curves on all datasets. Despite RF's dominance, other algorithms also showed close performance, suggesting that the choice of algorithm should be tailored to the specific data characteristics of the application system [2]. The field of anomaly detection in cybersecurity is increasingly vital due to the varied nature of cyber threats such as botnets, brute force, DoS/DDoS, port scans, MITM, SQL injection, and privilege escalation attacks. Traditional signature-based IDS methods, while effective for known threats, struggle against zero-day attacks and encrypted traffic from attackers. This highlights the need for advanced defense systems capable of predicting anomalous behavior through state-of-the-art ML algorithms, despite challenges in achieving high accuracy with low false alarm rates. The paper contributes to the cybersecurity domain by reviewing up-to-date datasets featuring modern attack scenarios and evaluating twelve ML algorithms through binary and multi-classification performance metrics. The research aims to guide the cybersecurity community and industry in selecting appropriate ML algorithms for tackling cybersecurity challenges [2]. The paper is structured to cover related work in ML-based anomaly detection, the methodology of the study, detailed experimental design and results, and conclusions with directions for future research.

This ongoing work focuses on further evaluating these methods on a smart grid dataset and assessing the efficiency of selected algorithms in terms of training and testing time.

A Machine Learning Approach to Anomaly Detection and Security Enhancement: This study based on Anton et al., 2021 addresses the escalating issue of cyber attacks on industrial enterprises, particularly focusing on industrial control systems (ICS) which have been increasingly targeted since their inception in the 1970s. Unlike typical IT systems, these industrial Operational Technology (OT) systems directly impact the physical world and often operate on outdated, hard-to-update technologies, making them vulnerable to attacks. This vulnerability is compounded by the advent of the Industrial Internet of Things (IIoT) and Industry 4.0, which integrate OT with IT systems, thereby increasing the risk of cyber attacks. Traditional security measures are inadequate for these specialized systems, necessitating advanced intrusion detection solutions [3]. In this research, analyze network data from industrial operations using machine learning and time series-based anomaly detection algorithms to identify cyber attacks. Two specific datasets were examined: one featuring Modbus-based gas pipeline control traffic and another with OPC UA-based batch processing traffic. The study primarily employs two machine learning algorithms, Support Vector Machines (SVM) and Random Forest, with Random Forest showing slightly better performance in detecting various attack categories. The process involves feature extraction and selection, as well as addressing missing data challenges common in real-world datasets. The research highlights that industrial networks, initially designed to be isolated and application-specific, are now more interconnected due to developments like IIoT, increasing their susceptibility to cyber threats. This interconnectivity, coupled with the lack of inherent security in many industrial communication protocols like Modbus and Profinet, significantly enlarges the attack surface. Historical incidents like the 2015 Ukrainian power grid blackout illustrate the potential consequences of successful cyber attacks on these systems [3]. This study's findings suggest that while machine learning techniques like SVM and Random Forest can detect up to 95% of attacks, there remains a risk of undetected threats, indicating the need for further enhancements in industrial cyber security measures. These techniques benefit from the predictable nature of industrial processes and the abundant data these environments generate, but they are not infallible. Therefore, a combination of advanced detection methods and robust security protocols is essential for safeguarding industrial networks against increasingly sophisticated cyber attacks.

Literature Gap: The current body of research on machine learning (ML) applications in cyber-security for industrial and smart grid environments reveals several notable gaps that warrant further exploration. Firstly, there is a distinct lack of studies focusing on the adaptation and optimization of ML techniques for specific industrial contexts. While general approaches to anomaly detection have been well-explored, each industry possesses unique operational characteristics and faces distinct types of cyber threats, thus necessitating more customized ML solutions. Tailoring these models to cater to the specific threat landscapes and data patterns of different sectors could significantly enhance their effectiveness. The real-time processing capabilities and scalability of these ML systems in industrial environments have not been sufficiently addressed [4]. Most current research emphasizes the accuracy of anomaly detection without adequately considering the importance of immediate threat response, which is critical in industrial settings. Future research should aim to develop ML models capable of not only accurately detecting anomalies but also doing so with minimal delay, thereby facilitating prompt responses to potential threats. Additionally, the scalability of these models in handling the complexities of large industrial networks is an area that remains underexplored. Integration with legacy systems presents another significant challenge. Many industrial environments still operate on outdated technologies that are not readily compatible with advanced ML-based cyber-security solutions. Research efforts should therefore focus on creating intermediary solutions, either software or hardware, that can seamlessly integrate these advanced detection techniques into older systems without necessitating extensive overhauls. There is a literature gap in addressing the robustness of these systems against more advanced and evolving cyber-attack strategies, such as polymorphic malware or AI-generated attacks. Developing ML algorithms that can adapt to and identify such sophisticated and changing attack patterns is crucial

[5]. This may involve exploring unsupervised learning or reinforcement learning approaches. The aspect of data privacy and security in the training and implementation of ML models for cyber-security has been relatively under-explored. In an era increasingly concerned with data breaches and privacy issues, it's imperative to research methods that ensure ML models are not only effective in threat detection but also robust against data leakage and compliant with privacy regulations.

Theoretical Framework

The integration of Machine Learning (ML) into network anomaly detection in industrial environments requires a comprehensive and nuanced theoretical framework. This framework must be adaptable, robust, and tailored to address the unique challenges of industrial networks. It should align with existing theories while contributing new insights to enhance cyber-security.

Core Principles and Assumptions: The foundational principles and assumptions of the framework are grounded in the recognition that industrial networks possess distinct characteristics, markedly different from conventional IT networks. This understanding is pivotal to the development of anomaly detection models tailored specifically for these unique environments. Acknowledging the specialized needs of industrial settings, the framework emphasizes the importance of creating solutions that are not just effective but also relevant to the specific operational and security challenges faced in these contexts [7]. This approach aligns with current literature's focus on industry-specific solutions and incorporates the dynamic, ever-evolving nature of cyber threats, ensuring that the models remain effective against new and sophisticated attack vectors.

Adaptive Machine Learning Models: The centerpiece of the framework is the deployment of adaptive machine learning (ML) models, designed to evolve dynamically in real-time. These models are adept at continuously learning from new and changing data, a feature essential for keeping pace with the ever-evolving landscape of cyber threats. Their adaptability is particularly crucial in combating advanced cyber-attacks such as polymorphic malware and AI-generated threats, which traditional static models might fail to detect [8]. By continually updating their parameters and learning new patterns of anomalies, these adaptive ML models offer a proactive defense mechanism, ensuring that the security measures in place are always one step ahead of potential threats.

Ensemble Techniques for Enhanced Robustness: The framework strategically integrates ensemble techniques, with a specific emphasis on employing Random Forests, to augment the overall robustness and precision of anomaly detection. By amalgamating diverse learning algorithms, this approach significantly enhances the reliability of the system in identifying anomalies. This integration plays a pivotal role in ensuring scalability and real-time processing capabilities, particularly in the complex and dynamic environments of industrial settings [9]. The synergy achieved through ensemble methods, notably Random Forests, contributes to a more resilient and accurate anomaly detection system, aligning with the framework's objectives of effective and scalable real-time processing.

Practical Application in Detecting Advanced Threats: The practical application of the framework's adaptive machine learning models is particularly evident in scenarios involving advanced threats like polymorphic malware. Unlike static models, these dynamic models are designed to continuously adjust and evolve in response to new and changing patterns of cyber threats. This adaptability ensures that the detection system remains effective over time, consistently identifying and neutralizing threats even as they evolve [10]. By adapting to the ever-changing landscape of cyber threats, these models provide a robust and resilient defense mechanism, crucial for maintaining cybersecurity in environments where threats are constantly developing and becoming more sophisticated.

Feature Engineering: The framework places significant emphasis on feature engineering, recognizing its pivotal role in enhancing the performance of ML models. By prioritizing the extraction of meaningful

information from network data, the framework ensures that the models are trained on relevant and high-quality features. This strategic focus on feature engineering aligns seamlessly with established theoretical approaches, reinforcing the importance of extracting pertinent information to optimize the effectiveness of anomaly detection models [11]. The integration of robust feature engineering practices is instrumental in elevating the overall quality and efficiency of the ML models within the proposed framework.

Figure 2: Theoretical Network

(Self-created in Ms Word)

Incorporating Deep Learning Architectures: The framework extends current trends by incorporating deep learning architectures, such as RNNs and CNNs, tailored for anomaly detection in industrial networks [11]. These architectures are adept at processing the sequential and spatial data patterns often found in network traffic.

Integration with Legacy Systems: Recognizing the challenge of outdated technologies in industrial environments, the framework proposes intermediary solutions for integrating advanced ML techniques with legacy systems [12]. This ensures broader applicability and reduces the need for extensive system overhauls.

Emphasis on Real-Time Processing Capabilities: The framework places a strong emphasis on real-time processing capabilities in machine learning (ML) models, highlighting the critical need for immediate anomaly detection and response in industrial environments. By prioritizing minimal latency in these systems, the approach ensures that potential threats are identified and addressed swiftly, mitigating the risk of extensive damage. In industrial settings, where even minor delays in detecting and responding to cyber threats can lead to significant operational disruptions, financial losses, or safety hazards, the ability of ML models to process and analyze data in real time is not just beneficial but essential [13]. This focus on speed and efficiency in threat detection is a key component of a robust cybersecurity strategy.

Robustness Against Sophisticated Attacks: The framework emphasizes the importance of robustness against sophisticated cyber-attacks, advocating for the development of machine learning (ML) algorithms capable of adapting to and recognizing complex and evolving attack patterns. This approach involves leveraging advanced techniques like unsupervised learning and reinforcement learning, which allow for a more dynamic and proactive response to cyber threats. By employing these methods, the framework aims to stay ahead of attackers who continuously refine their strategies. This is crucial in an era where cyber threats are becoming increasingly intricate and traditional static defense mechanisms

are no longer sufficient [14]. Such adaptive algorithms can significantly enhance cybersecurity measures, providing a more resilient defense against these advanced threats.

Data Privacy and Security : The theoretical framework places a significant emphasis on addressing the paramount concern of data privacy and security within the realm of machine learning (ML) model training and implementation. In the contemporary digital landscape, where data breaches and privacy infringements loom large, the framework advocates for robust methods. These methods are designed to fortify ML models against potential data leakage and to ensure strict compliance with evolving privacy regulations [15]. Recognizing the growing sensitivity surrounding personal and confidential information, this aspect of the framework aligns with the imperative need to instill trust and integrity in ML applications, particularly in sectors dealing with sensitive data such as healthcare.

This theoretical framework for integrating machine learning into network anomaly detection in industrial settings is both comprehensive and practical. It aligns with existing theories and addresses identified gaps by emphasizing adaptive ML models, ensemble methods, deep learning architectures, and the importance of feature engineering. It also proposes solutions for real-time processing, integration with legacy systems, defense against advanced attacks, and ensuring data privacy and security. This approach ensures the framework's relevance and effectiveness in addressing the complex challenges of network security in industrial environments.

Application of Theoretical Framework

The theoretical framework developed for integrating machine learning (ML) into network anomaly detection in industrial environments offers a roadmap for applying advanced cyber-security measures in real-world scenarios. Its application extends across various industrial sectors, addressing unique challenges and providing tangible benefits.

Implementing Adaptive Machine Learning Models: *Scenario Implementation:* In the context of a manufacturing plant, where the integrity of the Operational Technology (OT) network is paramount, the deployment of adaptive machine learning (ML) models marks a significant leap in enhancing cybersecurity [16]. These advanced ML models are not static; they are designed to continuously learn and evolve in response to the changing landscape of network data. This dynamic nature allows them to detect even the most subtle anomalies that could signify emerging cyber threats, including those that are new or evolving.

Implications: The implementation of adaptive ML models shifts the cybersecurity approach from reactive to proactive. Traditional security measures often involve responding to threats after they have occurred. In contrast, adaptive ML models provide an ongoing, real-time analysis of network activity, enabling them to identify potential threats before they can cause harm [17]. This continuous adaptation to new and emerging threat patterns significantly diminishes the risk posed by sophisticated cyber-attacks.

Utilizing Ensemble Techniques for Robust Anomaly Detection: *Practical Application:* For a utility company managing a smart grid system, the integration of ensemble methods such as Random Forests provides a comprehensive solution for anomaly detection. By aggregating a variety of algorithms, this method creates a multi-faceted detection system [18]. This enhanced system is not only more adept at identifying a broad spectrum of anomalies, ranging from subtle to obvious, but it also brings together the strengths of individual algorithms, thereby offering a more nuanced and comprehensive analysis of network data.

Benefits: The key advantage of employing ensemble techniques lies in their ability to minimize false positives and negatives. This precision in anomaly detection ensures that the utility company’s smart grid operates with high efficiency and minimal disruption [19]. By accurately identifying true threats

while avoiding overreaction to non-threatening anomalies, ensemble methods like Random Forests maintain the delicate balance required for smooth operation in complex utility networks.

Feature Engineering in Diverse Industrial Settings: *Real-World Use:* In a chemical processing plant, the application of feature engineering enables the identification of critical parameters that signal potential security breaches or operational anomalies [20]. By homing in on these key data points, machine learning models become more efficient and tailored to the unique environment of the plant.

Implications: This targeted approach significantly improves the accuracy of anomaly detection. In an industry where even minor deviations can lead to major safety hazards or production losses, such precision is crucial for maintaining operational integrity and ensuring the safety of both the facility and its personnel [21].

Incorporating Deep Learning for Complex Anomaly Patterns: *Application:* In the intricate ecosystem of an automotive assembly line, where a myriad of sensors and devices constantly interact, deploying deep learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) proves invaluable [22]. These advanced models are adept at parsing through and analyzing the vast volumes of data generated, identifying anomalies that are otherwise hard to detect.

Benefits: This deep learning approach excels at uncovering complex, subtle patterns that traditional anomaly detection methods may overlook. It offers a more nuanced, in-depth analysis, significantly enhancing the assembly line's security framework and ensuring a more comprehensive protection against sophisticated cyber threats [23].

Integrating with Legacy Systems in Industrial Environments: *Practical Implementation:* In a power plant operating on legacy systems, the creation of intermediary software offers a strategic solution. This software acts as a bridge, facilitating the integration of advanced Machine Learning (ML) solutions into the existing framework [24]. It does so without necessitating a complete overhaul of the current systems.

Implications: This approach enables the power plant to modernize its cybersecurity defense effectively. By integrating cutting-edge ML technologies with existing legacy systems, the plant can enhance its security measures while still preserving the value of its longstanding infrastructure investments [25]. This balance maintains operational continuity while bringing cybersecurity up to date.

Real-Time Processing for Immediate Threat Response: *Scenario Application:* In a high-stakes environment like a telecommunications network, the deployment of ML models capable of real-time anomaly detection is crucial. These models swiftly identify and address cyber threats as they arise [26]. This rapid response is essential in such a network where delays can lead to extensive system disruptions.

Benefits: The ability to respond instantaneously to threats is invaluable in maintaining seamless service continuity [27]. It helps avert potential financial losses and protects the company's reputation from the damaging impacts of prolonged service outages or data breaches.

Robust Defense Against Sophisticated Cyber-Attacks: *Real-World Use:* In the context of a financial institution's network, where security is paramount, the implementation of ML algorithms that are specifically designed to adapt and recognize new, sophisticated attack patterns is critical [27]. These advanced algorithms are capable of evolving alongside the ever-changing landscape of cyber threats, offering an agile and effective defense mechanism.

Implications: This approach significantly elevates the security posture of financial networks, safeguarding sensitive financial data against a broad spectrum of cyber threats [28]. By anticipating and responding to emerging attack methodologies, these systems play a crucial role in protecting financial assets and client information from the sophisticated tactics employed by modern cybercriminals.

Ensuring Data Privacy and Security in ML Implementations: *Application in Practice:* In healthcare organizations, where patient data is both sensitive and confidential, it's crucial that machine learning (ML) models are meticulously designed to prevent data leakage and comply with stringent privacy regulations [28]. This involves implementing robust security protocols and ensuring adherence to healthcare-specific standards like HIPAA.

Benefits: By prioritizing data security and privacy in ML implementations, healthcare organizations not only protect against potential cyber threats but also maintain compliance with legal and ethical obligations [30]. This approach is essential in preserving the trust and integrity of the healthcare system, ensuring that patient data remains confidential and secure.

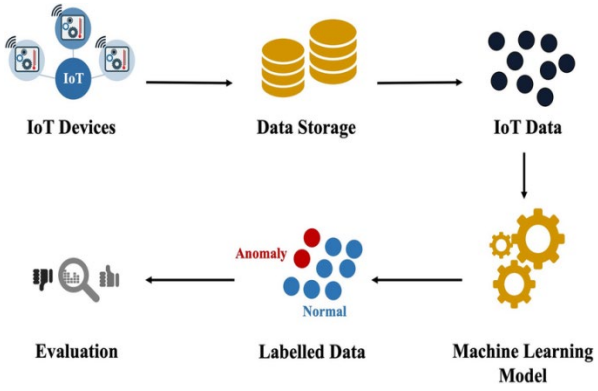

Figure 3: Machine Learning anomaly detection for Cybersecurity

(Source: https://www.researchgate.net/publication/354172900/figure/fig1/AS:1061648798318593@1630128206631/Machine-learning-workflow-for-anomaly-detection-in-IoT.png)

The application of the proposed theoretical framework in real-world scenarios across various industrial sectors demonstrates its versatility and effectiveness. By implementing adaptive ML models, utilizing ensemble techniques, and incorporating deep learning architectures, organizations can significantly enhance their anomaly detection capabilities. The framework's emphasis on real-time processing, integration with legacy systems, robust defense strategies, and data privacy ensures a comprehensive approach to network security. These applications not only provide a stronger defense against cyber threats but also bring operational efficiencies, maintain regulatory compliance, and ultimately protect the assets and reputation of organizations in an increasingly interconnected and digitalized industrial landscape.

Comparison with Existing Theories: In the world of finding weird things in computer networks and using machine learning to protect from harmful online attacks, many important ideas have been created. Each one adds special knowledge that helps people talk more about it every day. Set rules like Intrusion Detection Systems (IDS), Support Vector Machines (SVM), and Random Forests have helped us learn how to deal with strange activities in network spaces. Also, Deep Learning and Neural Networks are used for this task too [31]. These ideas have changed because of the ever-changing world of cyber threats. They give helpful ways to find and reduce possible dangers. Understanding and comparing these old ideas is very important for putting the new theory in this study into context. The paper wants to look at what's good and bad in old models. It will find out where current ways don't work well, plus explore how it can be creative. This side-by-side study not only makes our understanding better but also forms the base for creating a new system that tackles modern problems in finding odd things within networks [32]. In this way, one can look at old ideas. That helps to start a comprehensive discussion about how important and what future changes the new proposed idea could offer.

Overview of the Proposed Theoretical Framework: This study suggests a theory in an intelligent way to make network anomaly detection better for cybersecurity. This plan mixes old ways and new

tech. It uses things like planning features, adapting learning models from machines, and group practices together with deep brain designs to catch patterns quickly and study behavior in real time that lets it work well no matter what changes might come around. This framework uses parts from well-known theories and models to fix weaknesses in the old ways. It also takes advantage of their good points. The key part of the plan is a changing system that grows with new cyber threats. This makes it stay effective over time [33]. This section will comprehensively compare the proposed framework with existing theories, highlighting how it synergizes with established models and introduces novel elements to contribute to the evolving landscape of network anomaly detection. This comparative analysis aims to demonstrate the nuanced strengths and advancements this framework brings to the cybersecurity domain.

Comparing the theories

Differences: The proposed hypothetical framework veers from existing speculations in a few key perspectives, acquainting creative components with address impediments predominant in conventional models. In contrast to traditional Interruption Recognition Frameworks (IDS), our framework focuses on powerful variation through versatile ML models [34]. These models consistently develop in view of continuous criticism, empowering them to quickly conform to arising digital dangers. This flexibility is exemplified in situations where new assault designs arise, a feature where static models frequently battle. Besides, the joining of troupe procedures, especially Random Forests, separates our framework. While Random Forests are not novel, their application inside the setting of organization oddity recognition, close by deep learning structures, addresses a takeoff from particular model methodologies [56]. This group approach improves the power of our framework by consolidating the qualities of various models, alleviating the risk of false positives or negatives.

Substantial models delineate these distinctions. Consider a situation where a conventional IDS, depending entirely on static standards, neglects to distinguish a polymorphic malware variation because of its versatile nature [35]. Conversely, our framework, with its versatile models and group strategies, can observe the advancing examples of such dangers.

Similarities: Notwithstanding these distinctions, our hypothetical framework shares primary standards with existing speculations, encouraging a feeling of hypothetical union. The accentuation on highlight designing is a shared characteristic, recognizing the significance of separating significant data from network information. While our framework broadens this by incorporating progressed design methods, the common basic standard highlights a guarantee to improving the portrayal of organization traffic [36]. Furthermore, the utilization of ML models lines up with existing hypotheses, though with a nuanced approach. Where customary models might depend on solitary calculations, our framework expands upon this establishment by consolidating Adaptive ML models. This development guarantees similarity with laid-out strategies while presenting a layer of flexibility that is vital for taking care of dynamic cyber threats. The combination of deep learning models, like recurrent neural networks (RNNs) and convolutional neural networks (CNNs), reverberations the direction of existing speculations that embrace neural organization applications [37]. In any case, our framework expands this by fitting these structures explicitly for abnormality recognition, improving the comprehension of perplexing examples inside network traffic.

Aspects	Proposed Theoretical Framework	Existing Theories
Differences	**Adaptive Machine Learning Models:** The framework prioritizes dynamic adaptation through models that evolve in real-time, addressing emerging cyber threats [53].	**Static Rule-Based Systems:** Traditional models, like Intrusion Detection Systems, often rely on static rules, lacking adaptability to rapidly changing threats.
	Ensemble Techniques: Integration of ensemble methods, particularly Random Forests, enhances robustness by combining the strengths of different models.	**Singular Model Approaches:** Many existing theories rely on singular models, potentially leading to higher rates of false positives or negatives.

	Examples: In scenarios where polymorphic malware variants evolve, the adaptive nature of our framework ensures detection, contrasting with the limitations of static models.	**Scenario:** Traditional IDS might fail to detect evolving threats due to their static nature, highlighting limitations in adapting to dynamic attack patterns.
Similarities	**Foundational Principles:** Shared emphasis on feature engineering acknowledges the importance of extracting meaningful information from network data.	**Feature Engineering:** Both the proposed framework and existing theories recognize the foundational role of feature engineering in enhancing data representation [54].
	Use of Machine Learning Models: The framework aligns with existing theories by utilizing machine learning models, but with a nuanced approach.	**Machine Learning Applications:** Existing theories also leverage machine learning models, albeit potentially relying on singular algorithms.
	Integration of Deep Learning Architectures: Echoing existing trends, our framework incorporates RNNs and CNNs, tailoring them specifically for anomaly detection [55].	**Neural Network Applications:** Existing theories may also embrace neural network applications, but our framework tailors them for anomaly detection purposes.

Table 1: Comparing the proposed theoretical framework with existing theories

(Source: Self-created in MS Word)

While this proposed hypothetical framework acquaints particular components with tackle limits in existing speculations, it keeps a hypothetical union by utilizing essential standards imparted to customary models [37]. This union of development and coherence positions our framework as a forward-looking commitment to the developing scene of organization inconsistency discovery for cybersecurity.

Potential Synergies

The proposed hypothetical framework displays critical potential for cooperative energies with existing hypotheses in network peculiarity discovery, encouraging a cooperative methodology that exploits shared qualities. One vital area of cooperative energy lies in the coordination of versatile AI models, lining up with the standards of traditional Intrusion Detection Systems (IDS) [52]. By amalgamating the versatile idea of our framework with the fundamental standards of IDS, there exists a potential chance to improve the responsiveness to dynamic cyber threats, consequently alleviating the restrictions inborn in static rule-based frameworks. Group strategies, especially Random Forests, give one more road to collaboration. Consolidating the outfit approach of our framework with existing particular model methodologies makes an agreeable mix that works on in general strength. This cooperative methodology limits the risk of false positives or negatives, as the qualities of various models complete one another [38]. Additionally, the common accentuation on feature engineering and AI models lays out shared conviction for the mix. By blending progressed feature engineering procedures from our framework with the conventional utilization of AI models found in existing hypotheses, a more extensive and versatile peculiarity location framework can arise.

In synopsis, the likely collaborations between our proposed hypothetical framework and existing hypotheses offer a pathway to a comprehensive and strong peculiarity recognition arrangement. By recognizing shared view and coordinating key components, one imagines upgraded viability in defending organization conditions against advancing cybersecurity threats.

Applications and Implications

The examination between the proposed hypothetical framework and existing speculations divulges reasonable applications and suggestions for cybersecurity. Understanding the exchange between these hypotheses educates the advancement regarding more strong and versatile cybersecurity measures [51]. This incorporates the making of cutting edge peculiarity discovery frameworks able to do progressively adjusting to arising threats. The elevated flexibility adds to more viable cyber protection techniques. Moreover, the correlation educates the refinement regarding existing models, cultivating an aggregate development in peculiarity location strategies [39]. The ramifications stretch out to further developed

flexibility against complex cyber threats, giving an establishment to the nonstop upgrade of cybersecurity measures.

Critical Analysis

The similar investigation between the proposed hypothetical framework and existing speculations has yielded significant experiences, yet not without experienced difficulties. Ambiguities emerged, especially in measuring the presentation upgrades coming about because of the mix of versatile AI models and group procedures. Tending to these difficulties is crucial for the general progression of hypothetical grasping in the field [50]. Investigating strategic ambiguities permits specialists to refine assessment measurements and procedures, encouraging a more nuanced cognizance of the proposed framework's commitments. This basic examination underscores the significance of exploring difficulties constantly chasing refining and upgrading hypothetical models in network anomaly detection for cybersecurity [40]. By tending to these vulnerabilities, analysts add to the development and development of the hypothetical scene, laying the basis for additional complex and significant ways to deal with cybersecurity measures.

Taking everything into account, the near investigation between the proposed hypothetical framework and existing speculations has uncovered huge hypothetical ramifications, difficulties, and roads for refinement. The fuse of versatile AI models, troupe strategies, and high level component designing proposes the potential for a dynamic and strong anomaly detection framework. The affirmation of difficulties in measurement, coordination, and information protection highlights the intricacies intrinsic in progressing hypothetical models [41]. Perceiving the exchange between our framework and existing hypotheses is urgent for consistent improvement. Resulting segments will additionally dig into commonsense applications and future headings, flawlessly expanding upon the laid out hypothetical establishment in this near examination.

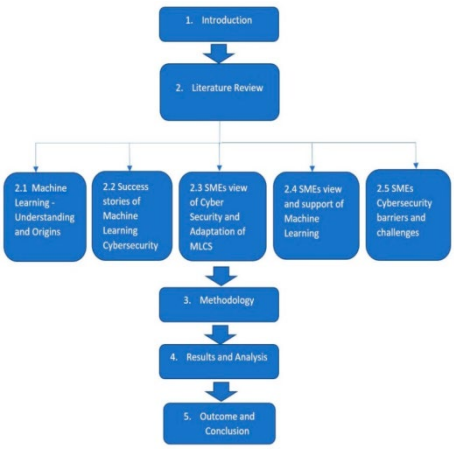

Figure 4: Machine Learning in Cybersecurity

(Source: https://www.mdpi.com/computers/computers-10-00150/article_deploy/html/images/computers-10-00150-g001.png)

Discussion

The proposed hypothetical framework envelops key parts, for example, adaptive machine learning models, ensemble techniques, and high level element designing. This exhaustive methodology plans to improve network anomaly detection for cybersecurity. In this part, the center movements to deciphering the hypothetical ramifications of this framework inside the predefined setting. By inspecting the hypothetical underpinnings, it plan to explain how the joining of these parts adds to the hypothetical scene of anomaly detection [42]. This investigation dives into the possible headways and commitments

the framework offers to the more extensive field of cybersecurity, making way for a nuanced comprehension of its hypothetical ramifications.

Interpretation of Theoretical Implications

Adaptive Machine Learning Models: Putting adaptive machine learning models in the framework has deep theory meanings. By using change easily, these ways greatly make the system better at dealing with new cyber dangers that come up. This ability makes a theory for an advanced unusual event finder system. It fits well with changing attack ways and protects us better from future cyber problems.

Ensemble Techniques: By adding in group methods, especially including Random Forests, it helps with important theory progress. Different models that work together make the system stronger. They also help in reducing mistakes where something is wrongly called as right or right called wrong [43]. This team effort uses many different models together. It makes the whole system for finding strange things even better in a theoretical way. The theory helps build stronger and more accurate protection against complex online dangers.

Feature Engineering and Deep Learning Architectures: The importance of theory is deeply included in the big feature work and mixes deep learning designs inside this setup. These things show a big change in understanding difficult patterns of traffic on the internet. Using advanced methods in feature creation and adding neural network designs helps a lot with the ideas that make up theory. This helps us to better see complex patterns that show something is wrong [44]. This improves our understanding of the cybersecurity area about spotting unusual things online.

So, the plan to create a theory shows deep effects. It does this by combining smart learning computer models, team techniques, and improved ways of using features. The ability to change, strong performance, and improved understanding of complex patterns all together help develop the theory behind finding strange things in cybersecurity.

Challenges and Limitations

Quantifying Performance Gains: It is hard to measure how much better things get because of the plan. Looking at adaptive models and group methods makes things harder, which causes confusion about performance measures. These models can change easily, making it hard to set up common measures. This makes checking how well they work in finding strange things more difficult [45]. To face these problems, one needs a complete assessment system that takes into account how adaptable models change over time and the joint effect of group methods.

Integration Challenges: Adding flexible models and group methods into the current cybersecurity system creates big problems. Some problems or barriers might come up when trying to use a more advanced and smart way of finding unusual things. Old systems might be designed for set-up models, making them hard to use with the changing and teamwork ideas of the suggested structure. Winning at joining things requires thinking about old parts, making sure everything moves well, and keeping the system good for finding mistakes.

Data Privacy and Security Concerns: Problems with data privacy and safety worries are part of advanced feature development and deep learning. Dealing with private data during the process of finding unusual patterns has moral concerns. It's difficult to keep data safe while still looking at it all. This gets harder when using fancy methods too [46]. Dealing with these problems needs to use strong ways of keeping private information safe, make sure all good rules are followed and help openness when handling personal data. It should match the new ideas with what's right to build trust in using the strange event detection plan one wants for cybersecurity.

Potential Refinements and Extensions

Fine-Tuning Adaptive Models: Refinement Exploration

- Delve into potential refinements for fine-tuning adaptive machine learning models.
- Investigate strategies to optimize model parameters, enhancing adaptability to dynamic cyber threats.
- Consider leveraging ongoing advancements in machine learning research to enhance the precision and adaptability of these models further.

Enhancements to Ensemble Techniques: Extension Discussion

- Discuss potential extensions or enhancements to ensemble techniques within the framework.
- Explore the incorporation of newer ensemble methods, such as boosting algorithms or meta-learning approaches.
- Consider optimizing existing ensemble methods to improve their collective anomaly detection capabilities.

Addressing Data Privacy Concerns: Refinement Proposals:

- Propose potential refinements to address data privacy concerns associated with advanced feature engineering.
- Explore privacy-preserving techniques, such as federated learning or differential privacy, to safeguard sensitive information.
- Discuss alternative approaches that strike a balance between ensuring security and preserving the effectiveness of the anomaly detection models.

In the world of making adaptive models better, looking at improvements is very important for getting them ready to deal with changing online dangers. The constant improvements happening in machine learning research are a good place for studying new ways to make these smart models more accurate and quick. When thinking about improving group methods, the attention turns to making the system more powerful [47]. This means looking into new group methods or making existing ones better to increase their ability to find strange things together. Adding power tools or learning methods can make team techniques better. This is very exciting for improving how they work together.

Solving worries about data privacy is a key part of improving the suggested plan. Suggesting changes means looking at ways to keep information private like federated learning and differential privacy. This helps make sure that important details are safe from others who shouldn't see them [48]. It's also important to talk about other ways that both keep us safe and help make the model work. This needs to be done so one can match new ideas in theory with good judgment when it comes to keeping our data private.

In the end, it has shown important ideas and problems in a suggested method for better understanding. The ability to change of machine learning models, the teamwork power of group methods and how features are used show important new ideas. Problems with counting, combining and keeping data secure show the difficult parts that come from moving forward with ideas [49]. Fixing these problems is very important for improving how one knows about network anomalies to protect against cyber threats. By figuring out these complexities, the idea world is ready to change. This will make understanding cyber threats better and it gives a strong base for future improvements in detecting odd things.

Conclusion

The proposed framework's hypothetical commitments are highlighted by the urgent jobs of adaptive machine learning models, ensemble techniques, and high-level element designing. The versatility innate in the machine learning models fundamentally hoists the framework's responsiveness to dynamic digital threats. Ensemble techniques, especially the incorporation of Random Forests, contribute by amalgamating assorted model qualities, in this way improving the heartiness of peculiarity recognition. High level element designing, combined with the combination of profound learning models, gives a nuanced comprehension of complex examples inside network traffic. On the whole, these parts structure an exhaustive hypothetical establishment that advances network irregularity recognition for cybersecurity. The flexibility, cooperative strength, and refinement presented by the framework all in all upgrade the hypothetical scene, promising a more successful and dynamic way to deal with battling arising cybersecurity challenges.

Figure 5: AI in Cyber Security

Challenges Encountered and the Importance of Addressing Them: The theoretical investigation experienced remarkable difficulties, including the measurement of execution gains, joining intricacies, and concerns connected with information protection. Measuring the presentation gains of the proposed framework demonstrated multifaceted, given the powerful idea of versatile models and ensemble techniques. Joining intricacies emerged in adjusting the framework to existing cybersecurity foundation, possibly restricting its consistent reception. Information protection concerns, intrinsic in cutting edge highlight designing, require cautious thought to adjust security and model viability. Addressing these moves is of basic significance to refine and strengthen the proposed framework. Conquering these complexities guarantees the heartiness and appropriateness of the hypothetical model, propelling its capability to contribute fundamentally to arrange oddity recognition for cybersecurity.

Significance of the Proposed Theoretical Framework: The proposed theoretical framework remains as a significant commitment by really tending to winning holes in network irregularity recognition hypotheses. Its incorporation of adaptive machine learning models, ensemble techniques, and high-level component designing gives an all encompassing and nuanced way to deal with increase peculiarity recognition capacities. By handling these hypothetical holes, the framework contributes essentially to propelling the comprehension of machine learning's key job in reinforcing cybersecurity. It presents a more modern and versatile hypothetical model, offering bits of knowledge into dynamic digital threats that conventional strategies might disregard. The framework's importance lies in its capability to lift the hypothetical scene of irregularity recognition, giving a complete and versatile establishment to counter arising cybersecurity challenges. In doing as such, it refines existing hypotheses as well as contributes significantly to the developing comprehension of the advantageous connection between machine learning and cybersecurity.

Future Directions and Continued Research: Future research should focus on refining the theoretical framework by exploring novel avenues, such as optimizing adaptive machine learning models and incorporating advanced ensemble methods. Adapting theoretical approaches is crucial to addressing emerging cyber threats and the continual evolution of the cybersecurity landscape. The dynamic nature of cyber threats necessitates ongoing research to ensure the theoretical framework remains at the forefront of anomaly detection methodologies. This adaptability is essential for developing robust and resilient theoretical models that can effectively counter the evolving tactics employed by cyber adversaries, thereby enhancing the overall effectiveness of network anomaly detection in the face of ever-changing cybersecurity challenges.

Therefore, progressing theoretical advancements assume a vital part in reasonable applications for network oddity identification. The ceaseless development of hypothetical frameworks in cybersecurity is vital for adjusting to advancing threats. By remaining at the very front of hypothetical development, these frameworks guarantee a proactive and versatile way to deal with countering digital threats. Idealism for what's in store lies in the versatility and strength that continuous hypothetical headways bring, protecting organization protection from the dynamic and complex nature of arising cybersecurity challenges.

References

[1] Anton, Simon D. Duque, Sapna Sinha, and Hans Dieter Schotten. "Anomaly-based intrusion detection in industrial data with SVM and random forests." In 2021 International conference on software, telecommunications and computer networks (SoftCOM), pp. 1-6. IEEE, 2021.

[2] Elmrabit, Nebrase, Feixiang Zhou, Fengyin Li, and Huiyu Zhou. "Evaluation of machine learning algorithms for anomaly detection." In 2020 international conference on cyber security and protection of digital services (cyber security), pp. 1-8. IEEE, 2020.

[3] Kayode-Ajala, Olaolu. "Anomaly Detection in Network Intrusion Detection Systems Using Machine Learning and Dimensionality Reduction." Sage Science Review of Applied Machine Learning 4, no. 1 (2021): 12-26.

[4] Hariharan, Ayush, Ankit Gupta, and Trisha Pal. "Camlpad: Cybersecurity autonomous machine learning platform for anomaly detection." In Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 2, pp. 705-720. Springer International Publishing, 2020.

[5] Larriva-Novo, Xavier, Mario Vega-Barbas, Victor A. Villagra, Diego Rivera, Manuel Alvarez-Campana, and Julio Berrocal. "Efficient distributed preprocessing model for machine learning-based anomaly detection over large-scale cybersecurity datasets." Applied Sciences 10, no. 10 (2020): 3430.

[6 Dutta, Vibekananda, Michał Choraś, Marek Pawlicki, and Rafał Kozik. "A deep learning ensemble for network anomaly and cyber-attack detection." Sensors 20, no. 16 (2020): 4583.

[7] Mubarak, Sinil, Mohamed Hadi Habaebi, Md Rafiqul Islam, Farah Diyana Abdul Rahman, and Mohammad Tahir. "Anomaly Detection in ICS Datasets with Machine Learning Algorithms." Computer Systems Science & Engineering 37, no. 1 (2021).

[8] Sarker, Iqbal H. "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks." Internet of Things 14 (2021): 100393.

[9] Evangelou, Marina, and Niall M. Adams. "An anomaly detection framework for cyber-security data." Computers & Security 97 (2020): 101941.

[10] Sarker, Iqbal H., Yoosef B. Abushark, Fawaz Alsolami, and Asif Irshad Khan. "Intrudtree: a machine learning based cyber security intrusion detection model." Symmetry 12, no. 5 (2020): 754.

[11] Wang, Song, Juan Fernando Balarezo, Sithamparanathan Kandeepan, Akram Al-Hourani, Karina Gomez Chavez, and Benjamin Rubinstein. "Machine learning in network anomaly detection: A survey." IEEE Access 9 (2021): 152379-152396.

[12] Larriva-Novo, Xavier A., Mario Vega-Barbas, Víctor A. Villagrá, and Mario Sanz Rodrigo. "Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies." IEEE Access 8 (2020): 9005-9014.

[13 Nassif, Ali Bou, Manar Abu Talib, Qassim Nasir, and Fatima Mohamad Dakalbab. "Machine learning for anomaly detection: A systematic review." Ieee Access 9 (2021): 78658-78700.

[14] Kayode-Ajala, Olaolu. "Anomaly Detection in Network Intrusion Detection Systems Using Machine Learning and Dimensionality Reduction." Sage Science Review of Applied Machine Learning 4, no. 1 (2021): 12-26.

[15] Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." Computer Networks 188 (2021): 107840.

[17] Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey." The Journal of Defense Modeling and Simulation 19, no. 1 (2022): 57-106.

[18] Rekha, Gillala, Shaveta Malik, Amit Kumar Tyagi, and Meghna Manoj Nair. "Intrusion detection in cyber security: role of machine learning and data mining in cyber security." Advances in Science, Technology and Engineering Systems Journal 5, no. 3 (2020): 72-81.

[19] Delplace, Antoine, Sheryl Hermoso, and Kristofer Anandita. "Cyber attack detection thanks to machine learning algorithms." arXiv preprint arXiv:2001.06309 (2020).

[20] Mohammadi Rouzbahani, Hossein, Hadis Karimipour, Abolfazl Rahimnejad, Ali Dehghantanha, and Gautam Srivastava. "Anomaly detection in cyber-physical systems using machine learning." Handbook of big data privacy (2020): 219-235.

[21] Ferrag, Mohamed Amine, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." Journal of Information Security and Applications 50 (2020): 102419.

[22] Liu, Zhipeng, Niraj Thapa, Addison Shaver, Kaushik Roy, Xiaohong Yuan, and Sajad Khorsandroo. "Anomaly detection on iot network intrusion using machine learning." In 2020 International conference on artificial intelligence, big data, computing and data communication systems (icABCD), pp. 1-5. IEEE, 2020.

[23] Lam, Jordan, and Robert Abbas. "Machine learning based anomaly detection for 5g networks." arXiv preprint arXiv:2003.03474 (2020).

[24] Tufan, Emrah, Cihangir Tezcan, and Cengiz Acartürk. "Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network." IEEE Access 9 (2021): 50078-50092.

[25] Komisarek, Mikolaj, Marek Pawlicki, Rafal Kozik, and Michal Choras. "Machine Learning Based Approach to Anomaly and Cyberattack Detection in Streamed Network Traffic Data." J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 12, no. 1 (2021): 3-19.

[26] Ali, Wasim A., K. N. Manasa, Malika Bendechache, Mohammed Fadhel Aljunaid, and P. Sandhya. "A review of current machine learning approaches for anomaly detection in network traffic." Journal of Telecommunications and the Digital Economy 8, no. 4 (2020): 64-95.

[27] Alqahtani, Hamed, Iqbal H. Sarker, Asra Kalim, Syed Md Minhaz Hossain, Sheikh Ikhlaq, and Sohrab Hossain. "Cyber intrusion detection using machine learning classification techniques." In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1, pp. 121-131. Springer Singapore, 2020.

[28] Mokhtari, Sohrab, Alireza Abbaspour, Kang K. Yen, and Arman Sargolzaei. "A machine learning approach for anomaly detection in industrial control systems based on measurement data." Electronics 10, no. 4 (2021): 407.

[30] Li, Zhida, Ana Laura Gonzalez Rios, and Ljiljana Trajković. "Machine learning for detecting anomalies and intrusions in communication networks." IEEE Journal on Selected Areas in Communications 39, no. 7 (2021): 2254-2264.

[31] Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. Network anomaly detection: A machine learning perspective. Crc Press, 2013.

[32] Hwang, Ren-Hung, Min-Chun Peng, Chien-Wei Huang, Po-Ching Lin, and Van-Linh Nguyen. "An unsupervised deep learning model for early network traffic anomaly detection." IEEE Access 8 (2020): 30387-30399.

[33] Ferrag, Mohamed Amine, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." Journal of Information Security and Applications 50 (2020): 102419.

[34] Alqahtani, Hamed, Iqbal H. Sarker, Asra Kalim, Syed Md Minhaz Hossain, Sheikh Ikhlaq, and Sohrab Hossain. "Cyber intrusion detection using machine learning classification techniques." In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1, pp. 121-131. Springer Singapore, 2020.

[35] Hooshmand, Mohammad Kazim, and Doreswamy Hosahalli. "Network anomaly detection using deep learning techniques." CAAI Transactions on Intelligence Technology 7, no. 2 (2022): 228-243.

[36] Ifzarne, Samir, Hiba Tabbaa, Imad Hafidi, and Nidal Lamghari. "Anomaly detection using machine learning techniques in wireless sensor networks." In Journal of Physics: Conference Series, vol. 1743, no. 1, p. 012021. IOP Publishing, 2021.

[37] Sen, Jaydip, and Sidra Mehtab. "Machine learning applications in misuse and anomaly detection." Security and privacy from a legal, ethical, and technical perspective (2020): 155.

[38] Fotiadou, Konstantina, Terpsichori-Helen Velivassaki, Artemis Voulkidis, Dimitrios Skias, Sofia Tsekeridou, and Theodore Zahariadis. "Network traffic anomaly detection via deep learning." Information 12, no. 5 (2021): 215.

[39] Sarker, Iqbal H. "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective." SN Computer Science 2, no. 3 (2021): 154.

[40] Tyagi, Himani, and Rajendra Kumar. "Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches." Revue d'Intelligence Artificielle 35, no. 1 (2021).

[41] Saba, Tanzila, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, and Saeed Ali Bahaj. "Anomaly-based intrusion detection system for IoT networks through deep learning model." Computers and Electrical Engineering 99 (2022): 107810.

[42] Nassar, Ahmed, and Mostafa Kamal. "Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies." Journal of Artificial Intelligence and Machine Learning in Management 5, no. 1 (2021): 51-63.

[43] Huč, Aleks, and Denis Trček. "Anomaly detection in IoT networks: From architectures to machine learning transparency." IEEE Access 9 (2021): 60607-60616.

[44] Singh, Vivek Kumar, and Manimaran Govindarasu. "A cyber-physical anomaly detection for wide-area protection using machine learning." IEEE Transactions on Smart Grid 12, no. 4 (2021): 3514-3526.

[45] Shaukat, Kamran, Suhuai Luo, Vijay Varadharajan, Ibrahim A. Hameed, Shan Chen, Dongxi Liu, and Jiaming Li. "Performance comparison and current challenges of using machine learning techniques in cybersecurity." Energies 13, no. 10 (2020): 2509.

[46] Maseer, Ziadoon Kamil, Robiah Yusof, Nazrulazhar Bahaman, Salama A. Mostafa, and Cik Feresa Mohd Foozy. "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset." IEEE access 9 (2021): 22351-22370.

[47] Ullah, Imtiaz, and Qusay H. Mahmoud. "Design and development of a deep learning-based model for anomaly detection in IoT networks." IEEE Access 9 (2021): 103906-103926.

[48] Shaukat, Kamran, Suhuai Luo, Vijay Varadharajan, Ibrahim A. Hameed, and Min Xu. "A survey on machine learning techniques for cyber security in the last decade." IEEE access 8 (2020): 222310-222354.

[49] Kotenko, Igor, Igor Saenko, and Alexander Branitskiy. "Machine learning and big data processing for cybersecurity data analysis." Data science in cybersecurity and cyberthreat intelligence (2020): 61-85.

[51] Kavitha, S., and N. Uma Maheswari. "Network anomaly detection for NSL-KDD dataset using deep learning." Information Technology in Industry 9, no. 2 (2021): 821-827.

[52] Rashid, ANM Bazlur, Mohiuddin Ahmed, Leslie F. Sikos, and Paul Haskell-Dowland. "Anomaly detection in cybersecurity datasets via cooperative co-evolution-based feature selection." ACM Transactions on Management Information Systems (TMIS) 13, no. 3 (2022): 1-39.

[53] Naseer, Sheraz, Rao Faizan Ali, P. D. D. Dominic, and Yasir Saleem. "Learning representations of network traffic using deep neural networks for network anomaly detection: A perspective towards oil and gas IT infrastructures." Symmetry 12, no. 11 (2020): 1882.

[54] Ripan, Rony Chowdhury, Iqbal H. Sarker, Md Musfique Anwar, Md Hasan Furhad, Fazle Rahat, Mohammed Moshiul Hoque, and Muhammad Sarfraz. "An isolation forest learning based outlier detection approach for effectively classifying cyber anomalies." In Hybrid Intelligent Systems: 20th International Conference on Hybrid Intelligent Systems (HIS 2020), December 14-16, 2020, pp. 270-279. Springer International Publishing, 2021.

[55] Al-Turaiki, Isra, and Najwa Altwaijry. "A convolutional neural network for improved anomaly-based network intrusion detection." Big Data 9, no. 3 (2021): 233-252.

[56] Imran, Faisal Jamil, and Dohyeun Kim. "An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments." Sustainability 13, no. 18 (2021): 10057.