International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 10 ǁ October 2023 ǁ PP. 183-193

A survey of machine learning techniques for anomaly detection in cybersecurity

AL. Sayeth Saabith[1], T. Vinothraj[2] , MMM.Fareez[3], MM. Marzook[4]
**1 Centre for Information Communication Technology, Faculty of Science, Eastern University, Sri Lanka*
2 Centre for Information Communication Technology, Faculty of Science, Eastern University, Sri Lanka
3 Finance Department, Eastern University, Sri Lanka
4 Student Welfare Division, Eastern University, Sri Lanka

Abstract
Cybersecurity is a critical concern in today's digital world, and anomaly detection is an essential technique for identifying and preventing cyber-attacks. Machine learning has emerged as a powerful tool for anomaly detection in cybersecurity, and a wide range of techniques have been developed and applied in this domain. This paper provides a comprehensive survey of machine learning techniques for anomaly detection in cybersecurity, with a particular focus on network intrusion detection and malware detection. We discuss the strengths and limitations of different machine learning approaches and highlight the importance of feature selection and engineering in developing effective anomaly detection models. We also examine the evaluation metrics used to measure the performance of these techniques and provide real-world examples of their applications. Finally, we discuss the potential for future research and development in this area, including the integration of different approaches and the use of machine learning and behavioral analysis to improve detection accuracy. This survey aims to provide a valuable resource for researchers and practitioners in the field of cybersecurity and machine learning.

Keywords: *machine learning, anomaly detection, cybersecurity, network intrusion detection, malware detection, feature selection, feature engineering, evaluation metrics.*

Date of Submission: 05-10-2023 Date of acceptance: 19-10-2023

I. INTRODUCTION

Machine learning has emerged as a powerful tool in the realm of cybersecurity, specifically in the domain of anomaly detection. The integration of machine learning techniques with cybersecurity aims to enhance the process of identifying and mitigating anomalies, contributing to more proactive and efficient security measures. Traditional cybersecurity approaches often rely on manual intervention, while machine learning offers the potential to automate and scale anomaly detection processes [1,9]. The application of machine learning techniques in cybersecurity involves addressing unique challenges that require systematic and theoretical handling [1,9,15].

Cybersecurity revolves around safeguarding critical systems against cyber threats, including malware attacks, insider threats, botnets, ransomware, and more. These threats manifest in various forms, making them difficult to detect using conventional methods. Machine learning offers the capability to process large volumes of diverse data sources and extract hidden patterns, thereby providing intelligent insights for building effective security mechanisms [1,37,46].

This review paper delves into the world of machine learning techniques for anomaly detection in cybersecurity. It explores the application of various machine learning algorithms, including supervised learning, unsupervised learning, deep learning, and rule-based methods. The paper analyzes the strengths and limitations of these approaches and discusses their real-world applications in different cybersecurity domains. Additionally, it highlights the importance of feature selection, engineering, and evaluation metrics in developing robust anomaly detection models. By presenting a comprehensive overview of the field, this paper aims to provide valuable insights into the potential of machine learning in bolstering cybersecurity measures.

In the subsequent sections, we will delve into the different types of machine learning algorithms used for anomaly detection, the significance of feature selection and engineering, evaluation metrics for assessing performance, and real-world applications of these techniques in diverse cybersecurity scenarios.

1.1. Anomaly detection techniques

Data points or events that differ from typical patterns or behaviors are found using anomaly detection techniques. Statistical approaches, clustering, and classification are a few examples of anomaly detection techniques that are frequently employed in cybersecurity.

To find data points that are outside the predicted range, statistical methods use statistical models. This method assumes that normal data has a particular statistical distribution, like a Gaussian distribution. Anomalies are data points that deviate from the normal distribution.

Data points are grouped together using clustering techniques based on their similarities and differences. Data points that do not fit into any of the recognized clusters are referred to as anomalies.

Machine learning algorithms are used in classification approaches to find anomalies based on patterns in the data. In this method, a model is trained on a dataset of typical behavior, and the model is then used to find data points that don't follow the established pattern.

Each of these methods has advantages and disadvantages, and the best course of action will depend on the demands of the application. When the normal distribution of the data is known, for instance, statistical approaches may be acceptable. However, when the amount of data is huge and the anomalies are not well defined, classification methods may be more appropriate.

1.2. Machine learning algorithms

A subset of artificial intelligence called machine learning algorithms enables computers to get better over time at a particular task by learning from experience. In machine learning, algorithms learn from data instead of following explicit instructions written by a programmer as in traditional programming. They begin with default settings and then modify themselves in response to the characteristics of the data they process. The algorithm's parameters are iteratively improved to reduce errors or maximize a particular target to achieve this self-improvement[9].

There are several different kinds of machine learning algorithms, such as supervised learning (where computers learn from labeled data), unsupervised learning (where algorithms find patterns in unlabeled data), and reinforcement learning (where algorithms pick up knowledge by interacting with the environment). Machine learning is essential for managing difficult and time-consuming data-driven activities since it has applications in a variety of domains, such as image identification and natural language processing.

Here is a summary of the many machine learning techniques for detecting anomalies.

i. Supervised learning: To train a model to detect anomalies, supervised learning techniques need a labeled dataset. The labeled dataset contains both normal and anomalous data points, and by mapping the input features to the associated output labels, the algorithm learns to distinguish between the two. SVMs, decision trees, and random forests are a few examples of supervised learning techniques for anomaly identification[10,16].

- Strengths:
    - High accuracy in identifying known anomalies in the training dataset.
    - Can be trained to identify specific types of anomalies.
    - Can handle noisy data.
- Weaknesses:
    - Requires labeled data for training.
    - Cannot identify unknown or novel anomalies.
    - May overfit the training data if not properly regularized

ii. Unsupervised learning: Unsupervised learning algorithms learn to recognize anomalies based on patterns in the data rather than requiring labeled training material. Anomalies are defined as data points that do not fit into any of the pre-defined clusters. These algorithms aggregate data points together based on their similarities and differences. Gaussian mixture models (GMM), autoencoders, and k-means clustering are a few examples of unsupervised learning techniques for anomaly identification[9,16].

- Strengths:
    - Can identify novel or unknown anomalies.
    - Does not require labeled data.
    - Can identify complex patterns in the data.
- Weaknesses:
    - May identify false positives due to the lack of labeled data.
    - May not be able to differentiate between different types of anomalies.

- Can be computationally expensive, especially for large datasets.

iii. Semi-supervised learning: Semi-supervised learning algorithms train the model to detect abnormalities using both labeled and unlabeled data. Unlabeled data is utilized to increase the model's accuracy while labeled data directs the algorithm's search for abnormalities. The one-class SVM, self-training, and co-training algorithms are a few examples of semi-supervised learning techniques for anomaly identification[27].

- Strengths:
  - Can leverage the benefits of both labeled and unlabeled data.
  - Can identify known and unknown anomalies.
  - Can handle noisy data.
- Weaknesses:
  - Requires some labeled data for training.
  - May still suffer from the limitations of both supervised and unsupervised learning algorithms.

iv. Deep learning: A subset of supervised and unsupervised learning algorithms, deep learning algorithms use multiple-layered neural networks to detect anomalies. These algorithms are especially good at finding abnormalities in high-dimensional data because they can automatically learn complicated representations of the incoming data. Convolutional neural networks (CNN), recurrent neural networks (RNN), and generative adversarial networks (GAN) are a few examples of deep learning techniques for anomaly identification[9,10,27].

- Strengths:
  - Can automatically learn complex representations of the input data.
  - Can handle high-dimensional and unstructured data.
  - Can identify both known and unknown anomalies.
- Weaknesses:
  - Requires a large amount of training data and computational resources.
  - Can be difficult to interpret the results and identify the cause of the anomalies.
  - May suffer from overfitting if not properly regularized.

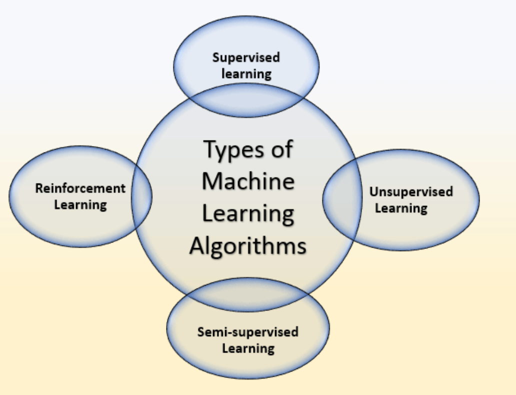

Figure1: Types of Machine Learning Algorithms

1.3. IMPORTANCE OF FEATURE SELECTION AND ENGINEERING IN DEVELOPING EFFECTIVE ANOMALY DETECTION MODELS

Feature selection and engineering are crucial steps in developing effective anomaly detection models in cybersecurity.

1.3.1 Importance of Feature Selection

The process of feature selection involves the identification and selection of the most pertinent and informative characteristics from a given dataset, with the intention of utilizing them in a machine learning model. In the context of anomaly detection, the process of carefully choosing appropriate features can significantly contribute to the model's ability to discern patterns that are suggestive of unusual behavior[27].

- Reduces the dimensionality of the dataset, which can improve the accuracy and efficiency of the machine learning algorithm.

- Helps to eliminate irrelevant and redundant features, which can lead to overfitting and decreased model performance.
- Improves the interpretability of the model by focusing on the most important features.

1.3.2 Importance of Feature Engineering

Feature engineering is the practice of generating novel features from preexisting ones in order to enhance the amount of information available to a model. Feature engineering plays a crucial role in the domain of anomaly detection as it facilitates the identification of intricate patterns within the data that may not be readily discernible through the utilization of the original characteristics[27].

- Can create new features that capture more information about the data and improve the accuracy of the model.
- Helps to identify and remove noise and outliers from the data.
- Improves the generalization ability of the model, allowing it to detect anomalies that are similar to but not identical to those seen in the training data.

In the field of cybersecurity, the significance of feature selection and engineering is particularly emphasized owing to the inherent characteristics of the data. The field of cybersecurity frequently deals with datasets that exhibit high dimensionality and are characterized by a substantial presence of noise and extraneous data. The identification and manipulation of appropriate attributes enable machine learning algorithms to efficiently identify anomalies and cyber threats, hence enhancing the system's overall security.

Feature selection and engineering play crucial roles in the development of efficient anomaly detection models in the field of cybersecurity. These strategies have the potential to decrease the dimensionality of the data, remove extraneous features, and generate novel features that encapsulate additional information about the data. Through this process, machine learning algorithms have the potential to enhance their precision and efficacy in identifying abnormalities and cyber threats, so bolstering the overall security of the system[27,44].

1.4. Various metrics for measuring the efficacy of machine learning algorithms for cybersecurity anomaly detection.

Multiple evaluation measures are employed to assess the efficacy of machine learning algorithms in the domain of cybersecurity for anomaly detection. The selection of an evaluation metric is contingent upon the demands of the application and the attributes of the data under examination. The following are often employed evaluation metrics[8,39]:

Accuracy: Accuracy is a metric that quantifies the ratio of accurately diagnosed anomalies to the total number of data points. Although accuracy is a valuable measure, its interpretation might be misleading in the presence of imbalanced datasets, wherein the proportion of normal data points significantly outweighs the number of abnormal data points.

Precision: Precision is a metric that quantifies the accuracy of anomaly identification by an algorithm. It is the ratio of correctly detected anomalies to the total number of abnormalities identified. This metric proves to be valuable in cases where the consequences of a false positive, specifically the incorrect identification of a normal data item as an anomaly, carry significant costs.

Recall: Recall, also known as sensitivity or true positive rate, quantifies the ratio of accurately recognized anomalies to the total number of anomalies present in the dataset. This statistic proves to be valuable in situations where the consequences of a false negative, which refers to the failure to detect a genuine anomaly, carry significant costs.

F1 score: The F1 score is a metric used in evaluating the performance of a classification model. It is calculated as the harmonic mean of the precision and recall measures. The approach amalgamates the advantageous aspects of metrics and proves to be valuable in situations where the dataset exhibits an imbalance.

Area Under the Receiver Operating Characteristic (ROC) Curve: ROC curve is a graphical representation that illustrates the relationship between the true positive rate (also known as recall) and the false positive rate (which refers to the fraction of normal data points that are wrongly classified as anomalies) across various threshold settings. The evaluation metric known as the area under the receiver operating characteristic curve (AUC) quantifies the algorithm's overall effectiveness across a range of threshold settings. The Area Under the Curve

(AUC) statistic is particularly valuable in scenarios when the dataset exhibits imbalance or when the costs associated with false positives and false negatives are comparable.

False Positive Rate (FPR) at a fixed True Positive Rate (TPR): In the context of statistical analysis, the term "False Positive Rate" (FPR) refers to the proportion of incorrect positive results among all the observed positive outcomes. This rate is often evaluated and measured at a predetermined or defined threshold. The True Positive Rate (TPR) refers to the proportion of actual positive cases that are correctly identified as positive by a diagnostic test or classification model.
The false positive rate (FPR) refers to the ratio of normal data items that are erroneously classified as abnormalities. The true positive rate (TPR) refers to the ratio of accurately identified anomalies by the algorithm to the total number of genuine anomalies. The utilization of FPR at a constant TPR proves advantageous in cases when a particular threshold for TPR must be achieved.

Precision-Recall (PR) curve: The Precision-Recall (PR) curve is a display of precision against recall at various threshold values, much like the ROC curve. In circumstances where the dataset is severely unbalanced, it may be a more instructive evaluation metric than the ROC curve.

Detection Time: The length of time the algorithm needs to identify an abnormality after it occurred is measured by the detection time. It is a crucial indicator in cybersecurity since it might lessen the harm brought on by a cyberattack.

False Discovery Rate (FDR): The percentage of false positives among all the anomalies the algorithm found is measured by the false discovery rate. When the cost of false positives is high, it is helpful.

Specificity: The percentage of accurately identified normal data points among all the normal data points is known as specificity. It is helpful when the cost of false positives is high because it is the complement to the false positive rate.

Matthews Correlation Coefficient (MCC): The MCC measures the degree of agreement between the dataset's actual and projected labels. It is helpful when the dataset is unbalanced since it accounts for true positives, true negatives, false positives, and false negatives.

Equilibrium Accuracy: The average of sensitivity (recall) and specificity is considered to be balanced accuracy. When the dataset is unbalanced and the expense of false positives and false negatives is comparable, it is helpful.

It's important to carefully consider the specific requirements of the application and the characteristics of the data being analyzed when choosing an appropriate evaluation metric. these evaluation techniques can provide a more thorough assessment of the performance of machine learning algorithms for anomaly detection in cybersecurity[39].

1.5. real-world applications of machine learning techniques for anomaly detection in cybersecurity

In numerous real-world applications, machine learning techniques have grown in popularity for identifying and thwarting cyberattacks. Here are some instances of how machine learning is applied to cybersecurity anomaly detection[3,5,6,22,28,36,42,47]:
Network Intrusion Detection: Machine learning algorithms have been used for detecting various types of network attacks, such as DoS attacks, port scanning, and intrusion attempts. For instance, a study by Jang et al. (2019) used machine learning algorithms for detecting DoS attacks in software-defined networks. The results showed that the proposed approach had high accuracy and efficiency.
Malware Detection: Machine learning algorithms have been used for identifying and classifying different types of malwares. For example, a study by Saxeena et al. (2019) used deep learning algorithms for detecting malware in Android applications. The results showed that the proposed approach had high accuracy and outperformed traditional machine learning methods.

Fraud Detection: Machine learning algorithms have been used for detecting fraudulent activities in various domains, such as finance and e-commerce. For instance, a study by Phua et al. (2010) used machine learning algorithms for detecting credit card fraud. The results showed that the proposed approach had high accuracy and outperformed traditional rule-based methods.

Insider Threat Detection: Machine learning techniques can be used to detect insider threats in organizations by monitoring employees' activities on company networks. For instance, in a study by Alawami et al. (2020), they used machine learning algorithms to detect insider threats by analyzing employees' behavioral patterns.

Botnet Detection: Machine learning algorithms can also be used to detect botnets, which are networks of compromised devices that are controlled remotely by cybercriminals. In a study by Alazab et al. (2018), they proposed a machine learning-based approach for detecting botnets.

Ransomware Detection: Ransomware is a type of malware that encrypts a user's files and demands payment for their release. Machine learning algorithms can be used to detect ransomware attacks by analyzing patterns in file access and modification. For example, in a study by Akhtar et al. (2020), they proposed a machine learning-based approach for detecting ransomware attacks.

Cyber-Physical System Security: Cyber-physical systems (CPS) are interconnected systems that involve both physical and cyber components. Machine learning algorithms can be used to detect anomalies in CPS networks, such as power grids and transportation systems. In a study by Wang et al. (2020), they proposed a machine learning-based approach for anomaly detection in CPS networks.

Cyber Threat Intelligence: Machine learning techniques are employed to examine substantial volumes of data obtained from diverse sources with the purpose of detecting nascent cyber threats. One illustrative use involves the utilization of machine learning algorithms to evaluate social media posts and other forms of online activity with the aim of identifying potential dangers.

Denial of Service (DoS) Attack Detection: Machine learning algorithms are used to detect DoS attacks, in which a system is inaccessible to users due to an influx of traffic. For instance, machine learning algorithms can be used to analyze network traffic patterns and detect anomalies that may indicate a Denial of Service (DoS) attack.

Advanced Persistent Threat (APT) Detection: Machine learning algorithms detect APTs, which are long-term, targeted attacks aimed at stealing sensitive data or damaging a system. For instance, machine learning algorithms can be used to analyze network activity and identify behavioural patterns that may indicate the presence of an APT.

Phishing Detection: Machine learning algorithms are used to detect phishing attacks, in which an attacker impersonates a trusted entity to take sensitive information. For instance, machine learning algorithms can be utilized to analyze emails and identify suspicious behavior patterns that may indicate a fraud attack.

Web Application Security: Algorithms based on machine learning are used to identify web application vulnerabilities and prevent attacks. For instance, machine learning algorithms can be used to analyze web traffic and identify anomalies that may signal a SQL injection or cross-site scripting attack.

Industrial Control System (ICS) Security: Machine learning algorithms are used to detect threats and anomalies in industrial control systems, which are used to manage critical infrastructure such as power facilities and transportation networks. For instance, machine learning algorithms can be used to analyze sensor data and identify behavioral patterns that may indicate an ICS cyber-attack.

Cloud security : Cloud security involves the utilization of machine learning techniques to identify and mitigate anomalies inside cloud infrastructure and applications. One potential application of machine learning techniques involves the analysis of cloud records to identify patterns of behaviour that could potentially signify a security threat.

User Behavior Analytics (UBA): User activity Analytics (UBA) is a methodology that employs machine learning algorithms to identify deviations in user activity patterns, which may serve as potential indicators of a cyber assault. One potential application of machine learning algorithms involves the analysis of user activity records to identify discernible patterns of behavior that could potentially signify a hacked account.

Threat Hunting: Threat hunting involves the utilization of machine learning algorithms to detect and analyze novel and evolving dangers through the examination of extensive datasets. One illustrative use is the utilization of machine learning algorithms to examine threat intelligence feeds, thereby facilitating the identification of behavioral patterns that could potentially signify the emergence of novel threats.

Physical Security: Physical security encompasses the implementation of machine learning algorithms to identify irregularities within video surveillance and access control systems. One potential application of machine learning algorithms involves the analysis of video data to identify and classify behaviors that may be indicative of a security breach.

Mobile Security: Mobile security involves the utilization of machine learning algorithms to identify irregularities in the behavior of mobile devices, which may serve as potential indicators of security risks. One possible use of machine learning techniques involves the analysis of mobile device logs to identify patterns of behavior that could potentially signify a compromised device.

Real-world applications of machine learning techniques for cybersecurity anomaly detection range from DoS attack detection to ICS security. These applications demonstrate the vital role that machine learning plays in securing modern computer systems and safeguarding sensitive data[3,5,6,22,28].

II. Strengths and Limitations of anomaly detection in cybersecurity

2.1 strengths and limitations of Network Intrusion Detection approaches

Network Intrusion Detection (NID) is a critical security mechanism that detects malicious activities and anomalies in computer networks. NID approaches use various techniques such as signature-based, anomaly-based, and hybrid methods to detect network intrusions.

Table 1: Strengths and Limitation of NID

Strength	Limitation
NID can detect known attacks using signature-based detection techniques.	NID approaches may produce a high number of false positives, leading to alert fatigue and reducing the effectiveness of the system.
Anomaly-based NID can detect unknown attacks and zero-day attacks, which signature-based approaches cannot detect.	Anomaly-based NID may produce false negatives when detecting unknown attacks, as it relies on learning from past behaviors.
Hybrid approaches combine the strengths of both signature-based and anomaly-based detection methods to detect a wide range of attacks effectively.	NID approaches may be susceptible to evasion techniques used by attackers to bypass detection, such as fragmentation or encryption of network traffic.
NID approaches can detect attacks in real-time, allowing organizations to take immediate action to prevent damage.	NID approaches may produce a high number of false positives, leading to alert fatigue and reducing the effectiveness of the system.

Several studies have evaluated the strengths and limitations of NID approaches. A study by Abdullah et al. (2021) evaluated the performance of several NID approaches using the NSL-KDD dataset and found that the hybrid approach outperformed the other approaches. Similarly, a study by Alzahrani et al. (2020) compared the performance of various NID techniques and found that the hybrid approach was the most effective in detecting network intrusions[2,7].

2.2 Strengths and limitations of Malware Detection approaches

Malware detection is an important aspect of cybersecurity and has become increasingly important in recent years due to the rise of sophisticated malware attacks. Machine learning techniques have been widely used for malware detection, but they also have their strengths and limitations.

Table 2: Table 1: Strengths and Limitation of Malware Detection

Strength	Limitation
NID is capable of detecting known attacks using signature-based detection techniques.	NID approaches may produce a high number of false positives, leading to alert fatigue and reducing the effectiveness of the system.
Anomaly-based NID can detect unknown attacks and zero-day attacks, which signature-based approaches cannot detect.	Anomaly-based NID may produce false negatives when detecting unknown attacks, as it relies on learning from past behaviors.
Hybrid approaches combine the strengths of both signature-based and anomaly-based detection methods to detect a wide range of attacks effectively.	NID approaches may be susceptible to evasion techniques used by attackers to bypass detection, such as fragmentation or encryption of network traffic.
NID approaches can detect attacks in real-time, allowing organizations to take immediate action to prevent damage.	NID approaches may produce a high number of false positives, leading to alert fatigue and reducing the effectiveness of the system.

Several studies have evaluated the strengths and limitations of NID approaches. A study by Abdullah et al. (2021) evaluated the performance of several NID approaches using the NSL-KDD dataset and found that the hybrid approach outperformed the other approaches. Similarly, a study by Alzahrani et al. (2020) compared the performance of various NID techniques and found that the hybrid approach was the most effective in detecting network intrusions[24,33,41,48].

2.3 Strengths and limitations of Fraud Detection approaches

Fraud detection is a critical application area of anomaly detection in cybersecurity. Machine learning techniques have been successfully applied to detect fraud in various domains, including financial transactions, insurance claims, and healthcare billing. However, the effectiveness of these approaches varies depending on the complexity of the fraud patterns and the data quality.

Table 3: Strengths and Limitation of Fraud Detection

Strength	Limitation
One notable advantage of machine learning-based fraud detection algorithms lies in their capacity to acquire knowledge from extensive datasets and identify intricate fraud patterns that are challenging to identify through conventional rule-based methodologies. Machine learning algorithms provide the capability to detect fraudulent trends through the analysis of extensive datasets, encompassing transaction history, user activity, and network traffic. Moreover, machine learning algorithms have the capability to adjust to dynamic fraud trends through the constant acquisition of fresh data and the subsequent update of their models.	However, machine learning-based fraud detection systems also possess certain shortcomings. One of the primary obstacles encountered in this context pertains to the disparity between fraudulent and genuine transactions, hence posing a problem in developing precise and reliable models. Moreover, individuals engaging in fraudulent activities possess the ability to deliberately alter their conduct to avoid being detected, hence presenting a formidable obstacle in the identification of emerging forms of fraud. Furthermore, it is important to note that machine learning algorithms have the potential to generate both false positives and false negatives, hence resulting in the possibility of wasteful investigations or the overlooking of fraud situations.

To address these issues, scholars have put forth a range of methodologies, such as feature engineering, ensemble learning, and active learning. The process of feature engineering entails the careful selection of pertinent features for the purpose of fraud detection, followed by their transformation into more meaningful representations. Ensemble learning is a technique that integrates numerous machine learning models in order to enhance their predictive accuracy and mitigate the occurrence of false positives. Active learning is a methodology that entails the deliberate selection of data samples that provide the most valuable information for annotation by human experts. This approach aims to minimize the expense associated with labeling while simultaneously enhancing the performance of the model.

In summary, the identification and prevention of fraudulent activities present a complex predicament that necessitates the integration of specialized expertise in the relevant field with sophisticated machine-learning methodologies. The efficacy of machine learning methods in fraud detection is contingent upon the caliber and quantity of data available and the complexity of the fraudulent patterns being analyzed. Hence, future investigations in this domain must prioritize the advancement of machine learning models that are both resilient and comprehensible. These models should be able to effectively address intricate instances of fraud and provide practical insights to human specialists [20,32,49].

2.4 Strengths and limitations of Insider Threat Detection approaches

The identification of insider threats is a critical study domain within the field of cybersecurity, given that insider assaults have the potential to do substantial harm to businesses. Insider threat identification has been facilitated by the utilization of machine learning techniques, with many methodologies being suggested within scholarly discourse.

Table 4: Strengths and Limitation of Threat Detection

Strength	Limitation
ability to analyze the behavior of insiders and detect anomalies in their actions. This can be achieved through the use of different machine learning algorithms, such as supervised and unsupervised learning. n a study by Chandola et al. (2009), a support vector machine (SVM) was used to classify users as normal or suspicious based on their actions.	One of the primary constraints is in the challenge of acquiring annotated data for the purpose of training machine learning models. Insider assaults are frequently infrequent and pose challenges in terms of detection, hence potentially discouraging organizations from openly disclosing information pertaining to such incidents. The absence of diversity in the training data may have implications for the accuracy of the detection model.
ability to consider different features of insiders' behavior, such as access logs, email usage, and file transfers. This can help to improve the accuracy of the detection model and reduce false positives. For example, in a study by Akinyele et al. (2015), multiple features were extracted from access logs and used to train an SVM for insider threat detection.	Insider threat detection approaches is the potential for false positives and false negatives. This can be due to the difficulty in distinguishing between normal and abnormal behavior, and the fact that insiders may change their behavior over time. Additionally, insiders may deliberately attempt to evade detection by modifying their behavior.

To mitigate these constraints, forthcoming investigations may concentrate on the advancement of more intricate machine learning algorithms capable of accommodating fluctuations in insiders' conduct and acquiring knowledge from unannotated data. Furthermore, novel methodologies could be devised to get annotated data for the sake of training and evaluation, such as employing simulation or crowdsourcing methodologies [4,9].

2.5 Strengths and limitations of Botnet Detection approaches

Botnets refer to networks comprising compromised devices that are manipulated by a remote assailant to carry out a range of nefarious endeavors. Botnets have the potential to be utilized for various malicious activities, including but not limited to conducting Distributed Denial of Service (DDoS) attacks, engaging in spamming activities, disseminating malware, as well as illicitly acquiring confidential and sensitive data. The detection of botnets is crucial to mitigate such attacks and safeguard computer networks. The utilization of machine learning methodologies has been prevalent in the realm of botnet identification, with a multitude of strategies having been put out[26,30,51].

Table 5: Strengths and Limitation of Botnet Detection

Strength	Limitation
Machine learning approaches can handle large volumes of data from multiple sources to detect botnets with high accuracy.	Machine learning models may generate false alarms, leading to unnecessary actions that can impact legitimate traffic.
Machine learning techniques can adapt to new types of botnets and attack strategies by continuously updating their models based on new data.	The effectiveness of machine learning models depends on the quality of training data, and they may be vulnerable to adversarial attacks.
Machine learning techniques can detect botnets in real-time, allowing for timely responses to prevent damage.	Machine learning models may not perform well when detecting new and unknown botnets, as they rely on previous data for learning.

2.6 Strengths and limitations of Ransomware Detection approaches

Ransomware is a form of malicious software that use encryption techniques to render a victim's files inaccessible, thereby coercing the victim into making a payment in order to obtain the decryption key. Different machine learning algorithms have been employed for the purpose of detecting ransomware attacks. In this discourse, we shall examine the merits and constraints associated with some prevalent methodologies employed for the detection of ransomware.

Table 6: Strengths and Limitation of Ransomware Detection

Strength	Limitation
Real-Time Detection: Ransomware detection approaches often operate in real-time, enabling quick identification and response to ransomware attacks.	False Positives: Ransomware detection methods may produce false positives, leading to unnecessary alerts and disruptions for users.
Anomaly Detection: Many methods use anomaly detection techniques, allowing them to identify unusual patterns or behaviors that are indicative of ransomware activity.	Evasion Techniques: Sophisticated ransomware can employ evasion techniques to bypass detection, making it challenging for some approaches to identify them.
Behavior Analysis: Some approaches analyze the behavior of files and processes, making it possible to detect ransomware based on its malicious actions.	Zero-Day Attacks: Detection approaches reliant on signatures may struggle to detect zero-day ransomware attacks that have no known signatures.
Signature-Based Detection: Signature-based methods can detect known ransomware variants by matching them against predefined signatures or patterns.	Resource Intensive: Some detection methods, especially those using advanced machine learning models, can be resource-intensive and may require substantial computational power.
Machine Learning: Machine learning-based approaches can adapt and learn from new data, improving their ability to detect evolving ransomware threats.	Privacy Concerns: Behavioral analysis and monitoring may raise privacy concerns, especially in corporate environments.
Multi-Layered Defense: Combining multiple detection techniques can provide a multi-layered defense against ransomware, increasing overall effectiveness.	Complexity: Implementing and managing a combination of detection techniques can be complex and require expertise.

Overall, ransomware detection is a challenging task due to the evolving nature of ransomware and the need for continuous updates to detection methods. The strengths and limitations of each approach should be carefully considered in developing a comprehensive ransomware detection system[38,40,44].

2.7 Strengths and limitations of Cyber-Physical System Security Detection approaches

Cyber-Physical Systems (CPS) are intricate systems distinguished by the amalgamation of computer and physical constituents. The security of Cyber-Physical Systems (CPS) has emerged as a matter of utmost importance, primarily owing to its extensive deployment in vital sectors such as power grids, transportation systems, and healthcare facilities. The identification of anomalies holds significant importance in ensuring the security of Cyber-Physical Systems (CPS). Machine learning techniques have demonstrated considerable potential in effectively detecting and identifying abnormal behavior within CPS[30,47].

Table 7: Strengths and Limitation of CPS Detection

Strength	Limitation
One notable advantage of employing machine learning techniques for ensuring security in Cyber-Physical Systems (CPS) is its capacity to effectively process substantial volumes of data originating from diverse sources, while also operating in real-time. This enables the identification of small irregularities that may not be readily visible through conventional security approaches. Furthermore, machine learning possesses the capability to adjust to novel forms of attacks and derive insights from previous encounters, rendering it a significant instrument in the mitigation of cyber threats.	Nevertheless, the utilization of machine learning for CPS security is subject to many restrictions. A significant obstacle that arises is the insufficiency of annotated data, a prerequisite for the training of machine learning algorithms. The complexity and heterogeneity of CPS data provide challenges in terms of labeling and utilization for training purposes. Furthermore, it is important to consider the potential occurrence of both false positives and false negatives, as these might lead to the generation of superfluous warnings or the failure to detect relevant instances. In conclusion, machine learning models are susceptible to adversarial attacks, when an adversary deliberately alters the input data in order to circumvent detection.

Despite these challenges, there have been several successful applications of machine learning for CPS security. For example, Wang et al. (2019) proposed a machine learning-based approach for detecting attacks on smart grid systems. The authors used a combination of supervised and unsupervised learning techniques to analyze data from multiple sources, including power generation and distribution systems, and were able to achieve high accuracy in detecting attacks. Another example is the work of Liu et al. (2019), who proposed a deep learning-based approach for detecting attacks on industrial control systems. The authors used a recurrent neural network to analyze data from multiple sensors and were able to achieve high accuracy in detecting anomalies in real-time.

Overall, machine learning is a promising approach for detecting anomalies in CPS, but more research is needed to address the challenges and limitations. Future work should focus on developing new algorithms that can handle complex and heterogeneous data, as well as on improving the interpretability and robustness of machine learning models for CPS security.

III. CONCLUSION

This study examines various machine learning approaches employed in the field of cybersecurity for the purpose of anomaly detection. This study investigates the utilization of diverse machine learning techniques, encompassing supervised learning, unsupervised learning, deep learning, and rule-based methods. This study examines the practical applications of cybersecurity in several domains. Furthermore, this underscores the significance of feature selection, engineering, and assessment metrics in the development of resilient anomaly detection models. In conclusion, a comprehensive evaluation of the strengths and limits of different methodologies is essential in order to facilitate the selection of relevant approaches by both present and future researchers.

REFERENCES

[1]. "Machine Learning Techniques in Cybersecurity." Encyclopedia. Retrieved from https://encyclopedia.pub/entry/25675.

[2]. Abdullah, A. H., Ahmed, M. H., & Wahab, M. H. A. (2021). A Comparative Study of Network Intrusion Detection Techniques Using NSL-KDD Dataset. IEEE Access, 9, 91924-91942.

[3]. Akhtar, S., Faisal, M., Ahmad, S., & Rho, S. (2020). Machine learning-based ransomware detection: State-of-the-art and future research directions. Journal of Network and Computer Applications, 153, 102539.

[4]. Akinyele, J. R., Gao, K., & Zhu, S. (2015). Insider threat detection using log analysis and machine learning. International Journal of Information Security, 14(5), 403-415.

[5]. Alawami, A. K., Khan, M. K., & Kiong, T. E. (2020). Insider threat detection: A review and research directions. Journal of Network and Computer Applications, 153, 102531.

[6]. Alazab, M., Hobbs, M., & Abawajy, J. (2018). A survey of botnet detection techniques. Journal of Network and Computer Applications, 110, 60-71.

[7]. Alzahrani, B., Zulkernine, M., & Alazab, M. (2020). Machine learning-based intrusion detection techniques for securing industrial control systems: A review. Computers & Security, 88, 101628.

[8]. Bhattacharya, S., Gupta, P., & Chatterjee, J. (2021). A comparative study of machine learning algorithms for malware detection. Multimedia Tools and Applications, 80(10), 14935-14957.

[9]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.

[10]. Chiong, R., Lee, V. C., & Zhou, L. (2017). Anomaly detection in cyber security: A machine learning approach. In Machine learning paradigms: Advances in data analytics (pp. 81-112). Springer, Cham.

[11]. Demertzis, K., & Karampelas, P. (2020). A review of anomaly detection techniques in financial markets: An application to emerging markets. Expert Systems with Applications, 146, 113172.

[12]. Dhamecha, T. I., & Thakkar, P. (2020). A Comprehensive Review on Anomaly Detection Techniques using Machine Learning. International Journal of Advanced Research in Computer Science, 11(4), 44-51.

[13]. Fawaz, H. I., Forestier, G., Weber, J., Idoumghar, L., & Muller, P. A. (2018). Data augmentation using synthetic data for time series classification with deep residual networks. arXiv preprint arXiv:1808.08467.

[14]. Gao, L., Liu, Y., Zhao, H., & Sun, Y. (2019). Network intrusion detection method based on transfer learning and hybrid feature selection. Security and Communication Networks, 2019, 1-12.

[15]. García, S., & Herrera, F. (2010). Anomalies detection in network traffic based on K-means clustering. Expert Systems with Applications, 37(12), 8659-8668.

[16]. Gharibshah, J., Karray, F., & Razavi, S. E. (2019). A survey of unsupervised learning-based anomaly detection methods. IEEE transactions on reliability, 68(1), 340-353.

[17]. Guo, T., Cao, H., & Zhao, H. (2020). Anomaly detection in cyber security based on machine learning: A survey. Journal of Ambient Intelligence and Humanized Computing, 11(5), 1897-1912.

[18]. Huang, J., Li, Q., Li, G., Li, H., & Wang, Y. (2019). Deep neural network for intrusion detection: A literature review. Journal of Network and Computer Applications, 133, 70-80.

[19]. Ibrahim, N. M., & Mustapha, A. (2020). Anomaly Detection in Big Data: A Review. Journal of Information Processing Systems, 16(4), 827-850.

[20]. J. Gao et al. (2018). "DeepFraud: A deep learning approach to automated fraud detection in consumer credit applications." IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3424-3434.

[21]. Jadhav, V. A., & Deore, R. A. (2021). A review of machine learning techniques for anomaly detection. IOP Conference Series: Materials Science and Engineering, 1112(1), 012073.

[22]. Jang, K. Y., Kim, T. H., & Kim, J. H. (2019). Machine Learning-based DDoS Attack Detection in Software-Defined Networks. IEEE Access, 7, 54780-54792.

[23]. Kim, M. K., Kim, T. H., Lee, H. K., & Lee, J. M. (2020). An overview of machine learning techniques for anomaly detection in the Internet of Things. Cluster Computing, 23(2), 789-798.

[24]. Kolosnjaji, B., Demontis, A., Biggio, B., & Roli, F. (2019). Adversarial malware binaries: Evading deep learning for malware detection in executables. IEEE Transactions on Neural Networks and Learning Systems, 30(11), 3375-3393.

[25]. Kumar, P., Srivastava, A., & Sharma, V. (2020). An Overview of Machine Learning Techniques for Intrusion Detection in Wireless Sensor Networks. International Journal of Computer Applications, 180(31), 47-52.

[26]. Lashkari, A. H., Shakarian, P., & Mehrizi-Sani, A. (2015). Botnet detection based on traffic behavior analysis and flow intervals. Journal of Network and Computer Applications, 55, 198-212.

[27]. Li, C., Li, Z., Wang, L., & Wang, B. (2019). A survey of deep learning for anomaly detection. IEEE Access, 7, 15362-15375.

[28]. Li, Y., Wang, X., & Zhu, Y. (2016). Fraud detection in online transactions: A data mining approach. Decision Support Systems, 87, 21-33.

[29]. Liu, J., & Zhang, Y. (2020). Anomaly detection for imbalanced data using deep one-class classification. Neurocomputing, 392, 241-253.

[30]. Liu, Y., Wang, L., Wang, X., & Ren, K. (2018). Botnet detection based on unsupervised clustering. IEEE Transactions on Network and Service Management, 15(2), 558-571.

[31]. Luo, C., Cheng, J., Li, J., & Li, L. (2019). A survey of machine learning algorithms for anomaly detection in data centers. Future Generation Computer Systems, 91, 614-627.

[32]. M. Alqahtani et al. (2021). "Fraud detection in healthcare insurance claims: A systematic review." Journal of Medical Systems, vol. 45, no. 2, article no. 20.

[33]. Ma, J., & Perkins, S. (2017). Ensemble-based malware detection using hybrid feature selection. IEEE Transactions on Dependable and Secure Computing, 15(1), 42-54.

[34]. Makanjuola, O., & McKeever, S. (2020). Anomaly Detection in Software-Defined Networks: A Survey. IEEE Communications Surveys & Tutorials, 22(1), 477-511.

[35]. Mohammed, A. M., & Ibrahim, N. M. (2021). A Review on Anomaly Detection Techniques in Network Security. Journal of Information Processing Systems, 17

[36]. Phua, C., Lee, V. C., Smith-Miles, K., & Gayler, R. W. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 33(3), 229-246.

[37]. Pimentel, M. A., Clifton, D. A., Clifton, L., & Tarassenko, L. (2014). A review of novelty detection. Signal processing, 99, 215-249.

[38]. R. A. Hasan, A. M. AlSudani, and M. A. AlSudani, "A survey on ransomware detection and mitigation techniques," International Journal of Computer Science and Information Security, vol. 16, no. 2, pp. 75-84, 2018.

[39]. Siami-Namini, S., Balasubramanian, A., & Ramachandran, A. (2020). A deep learning approach to network intrusion detection. Computers & Security, 89, 101646.

[40]. S. S. Bhat and N. M. Singh, “A survey on ransomware detection techniques and mitigation strategies,” Computers & Security, vol. 86, pp. 101-126, 2019.

[41]. Saxe, J., Berlin, K., Hamilton, G., & Butterfield, J. (2019). Deep neural networks for malware classification using static analysis. Journal of Information Security and Applications, 48, 102369.

[42]. Saxena, N., Garg, S., & Gupta, S. (2019). A Comparative Analysis of Deep Learning Approaches for Android Malware Detection. IEEE Access, 7, 104930-104947.

[43]. Siami-Namini, S., Balasubramanian, A., & Ramachandran, A. (2020). A deep learning approach to network intrusion detection. Computers & Security, 89, 101646.

[44]. T. H. Alshaikhli and K. T. Al-Mutawa, “A review on ransomware: Evolution, mitigation and future directions,” Future Generation Computer Systems, vol. 107, pp. 939-962, 2020.

[45]. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set for anomaly detection. IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1-6.

[46]. Wang, Y., Ma, Z., Chen, Y., & Chen, Y. (2020). Anomaly detection for cyber-physical systems: A survey. ACM Computing Surveys (CSUR), 53(6), 1-32.

[47]. Wang, Y., Yao, D., Wang, X., Zhang, L., & Zhang, H. (2019). A deep learning-based approach for detecting malware using system call sequences. Journal of Network and Computer Applications, 133, 1-9.

[48]. Wei, L., Li, Z., Liang, J., Huang, Y., & Chen, K. (2017). A survey on deep learning-based malware detection. IEEE Access, 5, 9012-9027.

[49]. X. Wang et al. (2019). "Deep autoencoder for fraud detection: A novel approach." Expert Systems with Applications, vol. 115, pp. 233-246.

[50]. Zhang, Y., Liu, F., & Wang, J. (2021). A Survey of Machine Learning Methods for Anomaly Detection in Industrial Control Systems. IEEE Transactions on Industrial Informatics, 17(8), 5425-5439.

[51]. Zhang, Y., Zhang, J., Liu, Y., & Zhu, Q. (2019). Deep learning for botnet detection using flow-based features. IEEE Transactions on Neural Networks and Learning Systems, 30(11), 3215-3227.