Journal of Theoretical and Applied Information Technology

30th November 2023. Vol.101. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REAL-TIME CLOUD-BASED AUTOMATION FOR CYBER THREATS DETECTION AND MITIGATION WITH MACHINE LEARNING MODELS

YOUNES WADIAI[1], YOUSEF EL MOURABIT[2], MOHAMMED BASLAM[3], BOUJEMAA NASSIRI[4], YOUSSEF ELHABOUZ[5]

[1]TIAD Laboratory, Sciences and Technology Faculty, Sultan Moulay Slimane University, Morocco

[2]TIAD Laboratory, Sciences and Technology Faculty, Sultan Moulay Slimane University, Morocco

[3] TIAD Laboratory, Sciences and Technology Faculty, Sultan Moulay Slimane University, Morocco

[4]Sustainable Innovation and Applied Research Laboratory, Polytechnique School, International University of Agadir, Morocco

[5]IGDR UMR 6290 CNRS Rennes 1 University, Rennes, France

E-mail : [1]younes.wadiai@gmail.com, [2] y.elmourabit@usms.ma, [3]m.baslam@usms.ma, [4]nassi.bouj@gmail.com, [5]youssef.elhabouz@univ-rennes1.fr

ABSTRACT

Using Cloud Computing in the artificial intelligence field is a paramount tool applied in technology solutions nowadays to build strong machine learning models. Most Cloud solutions available in the technology market offer gigantic storage spaces with high computing performances that are easily accessible online via terminals where local machines cannot compete with the performance of these cloud resources. Machine learning algorithms are becoming increasingly popular in the field of cloud security, as they provide powerful tools for detecting and mitigating a wide range of cyber threats. However, the full exploitation of web service portals offered in these cloud platforms is still limited and it is applied mostly to gain access or retrieve data from databases stored in servers. Using cloud services is beneficial and can allow the automation of the process of building trained models in real-time. In this article, we propose the usage of Microsoft Azure Machine Learning Studio Web Service tool to train manly the Multi Class Neural Network model and other algorithms using the CSE-CIC-IDS2018 dataset. While the experiments are performed using the attributes from the predefined dataset, the feeding process is conducted by building, deploying, and running simulated real-time collected attributes from the IDS/IPS system.

Keywords: *Web Services, Cloud Computing, Machine Learning, Deep Neural Network, CSE-CIC-IDS2018 Dataset, Real-time Filtering, Synchronous Learning*

1. INTRODUCTION

Given the prevalence of cyberattacks that spread quickly and evolve dynamically, the usage of cloud technology for intrusion detection is a crucial tool for ensuring a safe and reliable production network. In order to create a machine learning model to spot web attacks, this paper demonstrates how to combine behavior monitoring and similarity search as a web service. Such a technique is often used in the financial transactions and cyber security fields, though, in our case, we attempt to incorporate real-time learning through autonomous model feeding.

Host Intrusion Detection Systems, also known as HIDS, and Network Intrusion Detection Systems, also known as NIDS, are the two main types of intrusion detection systems (IDSs) used in network security. The HIDS system is a host-based system installed on local machines such as software-based firewalls, and antiviruses. Whereas, NIDS is network-based equipment installed at the edge of each production network. The HIDS system mainly uses the signature to detect anomalies, while the NIDS uses checksums and behavior tracking to detect uncommon traffic. These two modes are the core protection mechanism for any network. In order to provide ultimate protection against web attacks, adopting prevention measures is the right action plan to protect enterprise networks from intrusions. The IDS/IPS systems can play this role through the implemented signature-based known attacks and a predefined list of threats, these

technologies are outdated with the evolving of new attack techniques and strategies. The objective of the proposed research is to introduce a new detection model based on a preventive method of IDS/IPS security to pre-detect attacks using behavior- tracking method which offers efficient protection when used in real-time to train a machine learning model thanks to the web services provided in the cloud computing [31] solutions such as Microsoft Azure in our study case.

In the article [1] we discussed the importance of using cloud performance to improve the accuracy of predictions and to build a strong learning model that can be implemented in an IPS or an IDS. This article discusses the usage of web service features in Microsoft Azure to feed the learning model with the information needed in the dataset. The logic behind this technique is to use a web portal to intake the information and exploit it in real time for ultimate efficiency and accuracy.

The article is presented as follows: In the first section, we will cite the related work to the research including a comparison of the various approaches to the issue. and then a section of our proposed approach that describes the technique used and the performed experiments followed by the results and discussion section to analyze the findings. And the last section is the conclusion of the article and outlines future work.

2. RELATED WORK

In this section, we discuss some of the recent research conducted in the field of artificial intelligence regarding the usage of cloud computing. Various approaches were used to take advantage of the cloud resources. For example, in [2], R. Zuech described how web attacks can be detected using random under-sampling (RUS) ratios and ensemble learners. With the usage of the CSE-CIC-IDS2018 dataset and the specialized infrastructure for data preparation, the test simulated a significant class imbalance that is present in the actual world for web attacks, and the experiment proved how the classification performance improved when applying the random under-sampling to the class imbalance to detect web attacks. On the other hand, in [3] Another approach was adopted by M. Khan which consisted of using a heterogeneous dataset to build a Convolutional Auto Encoder (Conv-AE) that allows the detection and the classification of unpredictable network attacks. The system offered a better accuracy rate compared to the traditional ID systems and also has fewer computation resources. With the usage of the NSL-KDD dataset F. Mustafa [4] applied six algorithms, and the results showed that the Random Forest algorithm got the top accuracy rate over the other models. However, Weka was used to train the models, which is based on the local machine performance that is limited compared to the cloud aptitudes.

V. Kanimozhi in [5] came up with a great approach, where the goal was to categorize Botnet attacks into one class. The suggested framework verifies the expected probability of various classifiers where the results are shown with accuracy and precision. Although, the execution phase remains a challenge because of the large amount of the treated data, which is why we adopted cloud performance to handle larger datasets in our research. I. Ajmal, in his paper [6] suggested using a hybrid IDS system along with machine learning in a cloud environment. The used dataset is the UNSW-NB15 and the proposed solution is an anomaly detection system that operates at the Cloud Hypervisor level and integrates the K-means clustering algorithm with the SVM classification algorithm. The used technique is promising but the results are poor compared to other supervised approaches since the retrieved accuracy from the SVM model still needs to improve.

K. Maheswari in [7] in his paper proposed the usage of the hybrid machine learning approach as called hybrid soft computing to be applied for web and cloud platforms using the KDD cup'99 and DARPA LLS DDoS-1.0 dataset. However, the proposed method misses some important attacks that threaten the network which raises the risks and weakens the model's performance.

In [8] Umer provided a review comparing the security algorithms used in cloud computing and edge computing. The paper suggested that the security challenges that come with edge technology present a serious threat to outdated nowadays cloud security solutions which makes it paramount to adopt newer detection techniques including machine learning and deep learning. In [9] Vanin demonstrated how the common security restrictions and the steeper rising need for computational analysis including data mining and blockchain require statistical analysis and demonstration of data that have imposed imperative adjustments for the current day cloud model. In this paper, it was explained how the current Intrusion Detection Systems are unable to preserve the integrity of the data with the evolving methods of hacking techniques.

The paper in reference [10] presents an overview of Intrusion Detection Systems (IDS) using a new classification system that categorizes IDSs based on various factors such as data source and detection method. Additionally, the paper compares various detection methods and data collection techniques. It includes a table summarizing Anomaly-based IDSs and analyzes IDSs in diverse settings such as data centers, backbone, Fog and Cloud Computing, and IoT models, along with the commonly used datasets and metrics. Lastly, the paper addresses the requirements and challenges associated with modern IDSs.

The article in [11] presents a novel deep learning technique for intrusion detection, which addresses the feasibility and sustainability concerns of current approaches in modern networks. The proposed technique includes a nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning and a deep learning classification model constructed using stacked NDAEs. The NDAE approach addresses these issues by learning a set of features that capture the relevant characteristics of network traffic and reduce the levels of human interaction required for intrusion detection. However, nonsymmetric architectures were used will enable the model to learn complex and nonlinear representations of the data, leading to higher accuracy levels.

Also, in [12] Vanin, discussed how machine learning algorithms have become popular to improve the efficiency and accuracy of IDS, especially with the growing threat of attacks on transmitted data due to the increasing use of the internet and communications. However, they still need improvement to increase the accuracy and reduce the false alarm rates. The text provides a taxonomy of different machine learning methods and a review of recent IDS using machine learning, highlighting their strengths and weaknesses.

In [13] Ndibwile aims to improve the efficiency of mitigation efforts against DDoS attacks by discussing the impact of performed DDoS attacks on the application layer of the OSI model. These attacks are capable of replicating legitimate traffic, avoiding IDS and IPS detection, which may also result in false positives. The paper proposes two contributions to mitigate the problem: first, a special anti-DDoS module that uses a trained classifier in a random tree machine-learning algorithm to generate rules and fine-tune existing IDS/IPS such as Snort; second, an approach that uses active authentication of traffic source at the Bait and Decoy server to identify false positives and route them to their intended destinations.

Also, in [14], The article discusses the increasing need for IDS and IPS systems due to the growing total number of Internet of Things devices that are linked and the corresponding increase in malicious activities. Jayalaxmi notes that while there are existing models for detecting and preventing intrusions, there is a lack of coherence and advancements in these models, and they have certain limitations that need to be addressed. In order to develop a more efficient security model, the author proposes a survey that analyzes risk factors using mapping techniques and presents a hybrid framework that emphasizes the use of Artificial Intelligence techniques for intrusion detection and prevention in IoTs. The survey provides a comparative analysis of these techniques, considering their feasibility, compatibility, challenges, and real-time issues, and aims to help industry and academia develop new security frameworks that are more effective and efficient.

In [15] Uğurlu discusses the importance of encryption in securing online communications and how it can be used by attackers to bypass security measures. The study used the ISCX VPN-NonVPN dataset and various machine learning algorithms such as XGBoost, decision tree, and random forest to test the proposed model and achieved a success rate of 94.53% in classifying encrypted traffic. Overall, the approach is promising in improving network security and protecting against potential attacks.

Garcia [16] proposed the creation of an IDS/IPS system called Dique, which is designed to detect and prevent denial of service (DoS) attacks. The system uses a deep learning algorithm to classify incoming packets as either benign or malicious `with Graphical User Interface to display captured and classified packet information in real-time. The suggested model achieves an accuracy of 0.99 on the CICDDoS2019 Dataset by using the Deep Feed Forward neural network algorithm. The document also describes an offensive system called Diluvio, which was used to validate the effectiveness of the Dique system. Diluvio includes seven different types of DoS attacks that can be selectively launched against a web server.

In [17] Singh explains that the old-school method to detect and prevent intrusions that are based on signatures is not effective against zero-day attacks. To address this, the author discusses the use of

different machine learning algorithms for intrusion detection including Naive Bayes, decision tree, and logistic regression for intrusion detection. The article describes the development of a new detection module that uses critical feature selection and is trained and tested with data obtained from the production's network. The outcomes demonstrate that the decision tree offers the greatest accuracy with a low misclassification rate of 98 percent.

Amrollahi [18] explains how traditional detection techniques are not effective with large amounts of data due to the complex and time-consuming analysis processes. He suggested the use of big data tools and techniques to assist in the analysis and storage of data in intrusion detection systems, reducing processing and training time. The article explained how machine learning has great benefits for intrusion detection systems and malware detection, but there is still some uncertainty about its application in this field. One of the biggest challenges is real-time malware detection, which requires advanced design and systems that can quickly identify the maliciousness of specific files, programs, and websites.

In [19] the paper discusses the use of machine learning in detecting malicious traffic in IoT networks, as many IoT devices are vulnerable to outside attacks due to their permanent network connection and limited computational power. The paper suggests that existing Intrusion Detection/Prevention Systems can utilize machine learning to protect networks that carry IoT traffic. The study conducted used the IoT-23 dataset and achieved high accuracy rates of up to 98 percent depending on the sub-dataset.

In [20] Karatay discusses the limits of traditional signature-based detection methods to detect anomalies in cyber security. And how machine learning techniques can detect the most subtle anomalies. Moreover, machine learning and deep learning models can adapt to changing patterns and behavior in the system, making them more effective and efficient in detecting new types of attacks. However, the author mentioned that machine learning and deep learning models are not foolproof and can also have their limitations. Like the detection of zero-day attacks that have not been previously encountered. Additionally, the accuracy of these models heavily relies on the quality of the data used to train them.

In [21] Sokolov discusses the application of machine learning techniques for analyzing cybersecurity threats in cloud environments, specifically for enterprise applications in telecommunications and the Internet of Things. The authors propose using Support Vector Machines, Neural Networks, and Deep Neural Networks to analyze monitoring data and combine classifier results based on performance weights. The proposed approach shows promising results and is suitable for enterprise-grade security applications.

Barik [22] highlights the increasing frequency of cyber-attacks and the growing field of cybersecurity. The usage of deep learning techniques, including convolutional neural networks, recurrent neural networks, and deep neural networks, in the realm of cybersecurity is examined in this article. The paper proposes a structure and runs a real-time laboratory setup to examine the captured data using various DL techniques. The experimental results demonstrate that DL techniques can effectively be applied in cybersecurity solutions, with the CNN model providing an accuracy of 98 percent.

Also, Ali [23] presents a systematic literature review of recent studies that focus on intrusion and malware detection using deep learning techniques in various environments, including Android, Windows, IoT, and the web. The author collected 107 papers from five well-known digital libraries and critically analyzed them to determine the types of threats being targeted, the platforms being used, and the accuracy of deep learning-based systems in detecting new security threats. The paper categorizes Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Deep Belief Networks (DBN), and Autoencoders as the most frequently used deep learning methods that have been effectively used in various application scenarios.

Amjad [24] discusses the challenges of intrusion detection in computer networks and IoT networks due to the exponential growth of data generation. Despite many systems that have been developed recently, conventional techniques are not effective enough to cope with progressive attacks. The study offers a thorough examination of deep learning-based intrusion detection, including a critical assessment of various performance indicators such as precision, recall, false alarm rate, detection rate, and accuracy.

Also, in [40] Ala Mughaid, highlights the need for wireless intrusion detection systems to improve data rate and security due to the network's increasing number of attacks. The suggested

methodology makes use of a variety of deep learning and machine learning techniques, including Decision Jungle, Multi-class Decision Forest, and Multi-class Neural Network to detect cyberattacks in 5G networks.

Agarwal [25] proposes the deep neural network feature selection-whale optimization algorithm (FS-WOA–DNN) as a novel approach that uses deep learning techniques to mitigate DDoS attacks. The method includes a pre-processing step where the input dataset is normalized using min-max normalization. The (FS-WOA) is then applied to choose the ideal combination of features to improve the classification procedure. The results show an accuracy of 95 percent in detecting DDoS attacks which is a significant improvement over conventional techniques that are not capable of detecting with high efficiency while minimizing the occurrence of false alarms.

The [26] paper discusses how Advanced Persistent Threat (APT) attacks are a growing concern in the cybersecurity world and require specialized intrusion detection mechanisms to protect against them, and suggests a hybrid IDS approach that covers both networks and hosts should be used. The hybrid approach uses both signature-based and behavioral-based detection mechanisms based on deep learning algorithms. Signature-based detection uses known patterns or signatures of malicious activities to identify threats, while behavioral-based detection looks for abnormal behavior patterns that may indicate an attack.

The [27] paper proposes a deep learning architecture for DoS attack detection as a part of an ongoing project to design and implement tools for the detection of 0-day threats. The proposed model is based on a deep autoencoder which is a semi-supervised task. The proposed solution achieved a detection accuracy of 95 percent on the CICIDS2017 dataset, indicating its potential for recognizing previously unseen or 0-day attacks.

[28] This paper proposes a hybrid approach for network intrusion detection that combines deep learning with machine learning methods. It uses Apache Spark for processing large amounts of network traffic data and employs stacked autoencoder networks for latent feature extraction, followed by several classification-based intrusion detection methods, and proves efficient and effective results in detecting network intrusions.

The [29] article provides a comprehensive overview of the literature on the use of deep learning in detecting DDoS attacks, identifying current research gaps, and suggesting future directions for study in the field of DDoS attack detection using deep learning including the generalization and robustness of deep learning models, the incorporation of diverse data sources, the development of hybrid models, and the investigation of adversarial attacks.

[30] The research introduces a Network Intrusion Detection System (NIDS) that utilizes a deep learning model. The system architecture comprises three main steps that start with a hybrid selection of features, followed by an evaluation rule, and ends with detection. Ayo applies various search approaches and characteristic analyzers to identify critical features for constructing a reliable classifier. The comparison of the system's performance with other related approaches indicates that the proposed technique achieves superior results with reduced false alarm rate, high accuracy rate, and decreased training and testing time.

In this section, we discuss some of the recent research conducted in the field of artificial intelligence regarding the usage of cloud computing. Various approaches were used to take advantage of the cloud resources. For example, in [2], R. Zuech described how web attacks can be detected using random under-sampling (RUS) ratios and ensemble learners. With the usage of the CSE-CIC-IDS2018 dataset and the specialized infrastructure for data preparation, the test simulated a significant class imbalance that is present in the actual world for web attacks, and the experiment proved how the classification performance improved when applying the random under-sampling to the class imbalance to detect web attacks. On the other hand, in [3] Another approach was adopted by M. Khan which consisted of using a heterogeneous dataset to build a Convolutional Auto Encoder (Conv-AE) that allows the detection and the classification of unpredictable network attacks. The system offered a better accuracy rate compared to the traditional ID systems and also has fewer computation resources.

With the usage of the NSL-KDD dataset F. Mustafa [4] applied six algorithms, and the results showed that the Random Forest algorithm got the top accuracy rate over the other models. However, Weka was used to train the models, which is based on the local machine performance that is limited compared to the cloud aptitudes.

V. Kanimozhi in [5] came up with a great approach, where the goal was to categorize Botnet attacks into one class. The suggested framework verifies the

expected probability of various classifiers where the results are shown with accuracy and precision. Although, the execution phase remains a challenge because of the large amount of the treated data, which is why we adopted cloud performance to handle larger datasets in our research. I. Ajmal, in his paper [6] suggested using a hybrid IDS system along with machine learning in a cloud environment. The used dataset is the UNSW-NB15 and the proposed solution is an anomaly detection system that operates at the Cloud Hypervisor level and integrates the K-means clustering algorithm with the SVM classification algorithm. The used technique is promising but the results are poor compared to other supervised approaches since the retrieved accuracy from the SVM model still needs to improve.

K. Maheswari in [7] in his paper proposed the usage of the hybrid machine learning approach as called hybrid soft computing to be applied for web and cloud platforms using the KDD cup'99 and DARPA LLS DDoS-1.0 dataset. However, the proposed method misses some important attacks that threaten the network which raises the risks and weakens the model's performance.

In [8] Umer provided a review comparing the security algorithms used in cloud computing and edge computing. The paper suggested that the security challenges that come with edge technology present a serious threat to outdated nowadays cloud security solutions which makes it paramount to adopt newer detection techniques including machine learning and deep learning. In [9] Vanin demonstrated how the common security restrictions and the steeper rising need for computational analysis including data mining and blockchain require statistical analysis and demonstration of data that have imposed imperative adjustments for the current day cloud model. In this paper, it was explained how the current Intrusion Detection Systems are unable to preserve the integrity of the data with the evolving methods of hacking techniques.

The paper in reference [10] presents an overview of Intrusion Detection Systems (IDS) using a new classification system that categorizes IDSs based on various factors such as data source and detection method. Additionally, the paper compares various detection methods and data collection techniques. It includes a table summarizing Anomaly-based IDSs and analyzes IDSs in diverse settings such as data centers, backbone, Fog and Cloud Computing, and IoT models, along with the commonly used datasets and metrics. Lastly, the paper addresses the requirements and challenges associated with modern IDSs.

The article in [11] presents a novel deep learning technique for intrusion detection, which addresses the feasibility and sustainability concerns of current approaches in modern networks. The proposed technique includes a nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning and a deep learning classification model constructed using stacked NDAEs. The NDAE approach addresses these issues by learning a set of features that capture the relevant characteristics of network traffic and reduce the levels of human interaction required for intrusion detection. However, nonsymmetric architectures were used will enable the model to learn complex and nonlinear representations of the data, leading to higher accuracy levels.

Also, in [12] Vanin, discussed how machine learning algorithms have become popular to improve the efficiency and accuracy of IDS, especially with the growing threat of attacks on transmitted data due to the increasing use of the internet and communications. However, they still need improvement to increase the accuracy and reduce the false alarm rates. The text provides a taxonomy of different machine learning methods and a review of recent IDS using machine learning, highlighting their strengths and weaknesses.

In [13] Ndibwile aims to improve the efficiency of mitigation efforts against DDoS attacks by discussing the impact of performed DDoS attacks on the application layer of the OSI model. These attacks are capable of replicating legitimate traffic, avoiding IDS and IPS detection, which may also result in false positives. The paper proposes two contributions to mitigate the problem: first, a special anti-DDoS module that uses a trained classifier in a random tree machine-learning algorithm to generate rules and fine-tune existing IDS/IPS such as Snort; second, an approach that uses active authentication of traffic source at the Bait and Decoy server to identify false positives and route them to their intended destinations.

Also, in [14], The article discusses the increasing need for IDS and IPS systems due to the growing total number of Internet of Things devices that are linked and the corresponding increase in malicious activities. Jayalaxmi notes that while there are existing models for detecting and preventing intrusions, there is a lack of coherence and advancements in these models, and they have certain limitations that need to be addressed. In

order to develop a more efficient security model, the author proposes a survey that analyzes risk factors using mapping techniques and presents a hybrid framework that emphasizes the use of Artificial Intelligence techniques for intrusion detection and prevention in IoTs. The survey provides a comparative analysis of these techniques, considering their feasibility, compatibility, challenges, and real-time issues, and aims to help industry and academia develop new security frameworks that are more effective and efficient.

In [15] Uğurlu discusses the importance of encryption in securing online communications and how it can be used by attackers to bypass security measures. The study used the ISCX VPN-NonVPN dataset and various machine learning algorithms such as XGBoost, decision tree, and random forest to test the proposed model and achieved a success rate of 94.53% in classifying encrypted traffic. Overall, the approach is promising in improving network security and protecting against potential attacks.

Garcia [16] proposed the creation of an IDS/IPS system called Dique, which is designed to detect and prevent denial of service (DoS) attacks. The system uses a deep learning algorithm to classify incoming packets as either benign or malicious `with Graphical User Interface to display captured and classified packet information in real-time. The suggested model achieves an accuracy of 0.99 on the CICDDoS2019 Dataset by using the Deep Feed Forward neural network algorithm. The document also describes an offensive system called Diluvio, which was used to validate the effectiveness of the Dique system. Diluvio includes seven different types of DoS attacks that can be selectively launched against a web server.

In [17] Singh explains that the old-school method to detect and prevent intrusions that are based on signatures is not effective against zero-day attacks. To address this, the author discusses the use of different machine learning algorithms for intrusion detection including Naive Bayes, decision tree, and logistic regression for intrusion detection. The article describes the development of a new detection module that uses critical feature selection and is trained and tested with data obtained from the production's network. The outcomes demonstrate that the decision tree offers the greatest accuracy with a low misclassification rate of 98 percent.

Amrollahi [18] explains how traditional detection techniques are not effective with large amounts of data due to the complex and time-consuming analysis processes. He suggested the use of big data tools and techniques to assist in the analysis and storage of data in intrusion detection systems, reducing processing and training time. The article explained how machine learning has great benefits for intrusion detection systems and malware detection, but there is still some uncertainty about its application in this field. One of the biggest challenges is real-time malware detection, which requires advanced design and systems that can quickly identify the maliciousness of specific files, programs, and websites.

In [19] the paper discusses the use of machine learning in detecting malicious traffic in IoT networks, as many IoT devices are vulnerable to outside attacks due to their permanent network connection and limited computational power. The paper suggests that existing Intrusion Detection/Prevention Systems can utilize machine learning to protect networks that carry IoT traffic. The study conducted used the IoT-23 dataset and achieved high accuracy rates of up to 98 percent depending on the sub-dataset.

In [20] Karatay discusses the limits of traditional signature-based detection methods to detect anomalies in cyber security. And how machine learning techniques can detect the most subtle anomalies. Moreover, machine learning and deep learning models can adapt to changing patterns and behavior in the system, making them more effective and efficient in detecting new types of attacks. However, the author mentioned that machine learning and deep learning models are not foolproof and can also have their limitations. Like the detection of zero-day attacks that have not been previously encountered. Additionally, the accuracy of these models heavily relies on the quality of the data used to train them.

In [21] Sokolov discusses the application of machine learning techniques for analyzing cybersecurity threats in cloud environments, specifically for enterprise applications in telecommunications and the Internet of Things. The authors propose using Support Vector Machines, Neural Networks, and Deep Neural Networks to analyze monitoring data and combine classifier results based on performance weights. The proposed approach shows promising results and is suitable for enterprise-grade security applications.

Barik [22] highlights the increasing frequency of cyber-attacks and the growing field of cybersecurity. The usage of deep learning techniques, including convolutional neural networks, recurrent neural networks, and deep neural networks, in the realm of cybersecurity is examined in this article. The paper proposes a structure and runs a real-time laboratory setup to examine the captured data using various DL techniques. The experimental results demonstrate that DL techniques can effectively be applied in cybersecurity solutions, with the CNN model providing an accuracy of 98 percent.

Also, Ali [23] presents a systematic literature review of recent studies that focus on intrusion and malware detection using deep learning techniques in various environments, including Android, Windows, IoT, and the web. The author collected 107 papers from five well-known digital libraries and critically analyzed them to determine the types of threats being targeted, the platforms being used, and the accuracy of deep learning-based systems in detecting new security threats. The paper categorizes Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Deep Belief Networks (DBN), and Autoencoders as the most frequently used deep learning methods that have been effectively used in various application scenarios.

Amjad [24] discusses the challenges of intrusion detection in computer networks and IoT networks due to the exponential growth of data generation. Despite many systems that have been developed recently, conventional techniques are not effective enough to cope with progressive attacks. The study offers a thorough examination of deep learning-based intrusion detection, including a critical assessment of various performance indicators such as precision, recall, false alarm rate, detection rate, and accuracy.

Also, in [40] Ala Mughaid, highlights the need for wireless intrusion detection systems to improve data rate and security due to the network's increasing number of attacks. The suggested methodology makes use of a variety of deep learning and machine learning techniques, including Decision Jungle, Multi-class Decision Forest, and Multi-class Neural Network to detect cyberattacks in 5G networks.

Agarwal [25] proposes the deep neural network feature selection-whale optimization algorithm (FS-WOA–DNN) as a novel approach that uses deep learning techniques to mitigate DDoS attacks. The method includes a pre-processing step where the input dataset is normalized using min-max normalization. The (FS-WOA) is then applied to choose the ideal combination of features to improve the classification procedure. The results show an accuracy of 95 percent in detecting DDoS attacks which is a significant improvement over conventional techniques that are not capable of detecting with high efficiency while minimizing the occurrence of false alarms.

The [26] paper discusses how Advanced Persistent Threat (APT) attacks are a growing concern in the cybersecurity world and require specialized intrusion detection mechanisms to protect against them, and suggests a hybrid IDS approach that covers both networks and hosts should be used. The hybrid approach uses both signature-based and behavioral-based detection mechanisms based on deep learning algorithms. Signature-based detection uses known patterns or signatures of malicious activities to identify threats, while behavioral-based detection looks for abnormal behavior patterns that may indicate an attack.

The [27] paper proposes a deep learning architecture for DoS attack detection as a part of an ongoing project to design and implement tools for the detection of 0-day threats. The proposed model is based on a deep autoencoder which is a semi-supervised task. The proposed solution achieved a detection accuracy of 95 percent on the CICIDS2017 dataset, indicating its potential for recognizing previously unseen or 0-day attacks.

[28] This paper proposes a hybrid approach for network intrusion detection that combines deep learning with machine learning methods. It uses Apache Spark for processing large amounts of network traffic data and employs stacked autoencoder networks for latent feature extraction, followed by several classification-based intrusion detection methods, and proves efficient and effective results in detecting network intrusions.

The [29] article provides a comprehensive overview of the literature on the use of deep learning in detecting DDoS attacks, identifying current research gaps, and suggesting future directions for study in the field of DDoS attack detection using deep learning including the generalization and robustness of deep learning models, the incorporation of diverse data sources, the development of hybrid models, and the investigation of adversarial attacks.

[30] The research introduces a Network Intrusion Detection System (NIDS) that utilizes a deep

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

learning model. The system architecture comprises three main steps that start with a hybrid selection of features, followed by an evaluation rule, and ends with detection. Ayo applies various search approaches and characteristic analyzers to identify critical features for constructing a reliable classifier. The comparison of the system's performance with other related approaches indicates that the proposed technique achieves superior results with reduced false alarm rate, high accuracy rate, and decreased training and testing time.

Table 1 serves as a Comparative Table of major cited work, offering a comprehensive overview of the datasets used and various metrics employed across the referenced studies. This table provides a valuable comparative analysis, shedding light on the key aspects of prior research in the field.

Table 1: Comparative Table of Major Cited Related Work.

Article /Study	***Algorithm***	***Dataset***	***Learning method***	***Accuracy***	***Precision***	***Recall***	***ROC***	***F-Measure***
[2]	Random Forest	CSE-CIC-IDS2018	supervised	0.99	0.99	0.99	-	0.99
[3]	Convolutional Autoencoder	NSL-KDD	unsupervised	0.99	0.98	0.99	-	0.99
[4]	Random Forest	NSL-KDD	supervised	0.98	0.97	0.98	-	0.97
[5]	gradient boosting	CSE-CIC-IDS2018	supervised	0.99	0.99	0.99	0.999	0.99
[6]	K-means & SVM	NSL-KDD	unsupervised	0.99	0.97	-	-	0.96
[7]	K-means	NSL-KDD	unsupervised	0.86	0.88	0.86	0.92	0.87
[9]	Random Forest	CICIDS-2017	supervised	0.98	0.98	0.98	-	0.97
[28]	Deep Convolutional Neural Network	NSL-KDD	supervised	0.98	0.98	0.98	0.998	0.98
[30]	Convolutional Neural Network	NSL-KDD	supervised	0.99	0.99	0.99	0.997	0.99
[28]	LSTM	UNSWNB15	supervised	0.98	0.98	0.99	0.999	0.98
[21]	Convolutional Neural Network	network traffic logs	supervised	0.98	0.98	0.98	0.998	0.98
[25]	CNN	network traffic logs	supervised	0.98	0.99	0.97	-	0.98

3. PROPOSED APPROACH

Since the publication, of our last article we developed a new methodology to refine and improve the detection of malicious traffic in IDS/IPS systems. The proposed approach aims to leverage new technologies and insights to enhance its efficacy in this exciting and rapidly evolving field.

We continue to work with the CSE-CIC-IDS2018 dataset from the Canadian Institute for Cyber Security. This dataset has over 80 collected attributes and was uploaded to the Azure Studio platform. By comparing the web service aspect and the manual feeding of the dataset. The previously built model gave us great results in terms of accuracy and prediction. However, the aim is to reach better accuracy by tuning the model and using other attributes of the dataset. The multiclass regression, multiclass neural network, and two class locally deep support vector machine [37] have a strong prediction system that we used in this experiment and combined with the web services feature in Azure Machine Learning Studio.

In this section, we introduce a novel approach to build a real-time machine learning model to be implemented in the IDS/IPS systems. The traditional method to detect anomalies in the network is the signature-based [41] solutions which is inefficient due to the ongoing changes of the

attack methods. Also, the trained model via machine learning algorithms is not efficient and do not provide high accuracy. The proposed method in our model is to have a real time learning model that collects incoming network packets, stores them in a dataset and then feed the model to be trained in real-time via web services portal we are using in our case which is Azure Web Services (AWS). AWS is used as it is a pioneer solution and an industry-leading machine learning operations (MLOps), open-source interoperability, and integrated tools, it reduces time to value. We are using this reliable platform in our experiment for highly performant machine learning applications and artificial intelligence.

This technique allows a simultaneous apprenticing from the incoming packets and allows the model to correct itself from false and true false alarms. The next sections will introduce the tools used to collect results from various performed experiments.

3.1 Azure Web Services

In this section, we will introduce the pivotal tool employed in this experiment, Azure Web Services, and shed light on how this innovative technique was harnessed to elevate the predictive model while also advancing the automation of the detection process. Azure Web Services, hosted within Azure Machine Learning Studio, represents a web-based platform that revolutionizes the landscape of machine learning by automating crucial processes, departing from the conventional approach of manual model construction and data feeding. The transformative power of this approach lies in its ability to accelerate results attainment while concurrently elevating accuracy levels.

In the context of building the learning model, Azure Machine Learning Studio takes center stage, leveraging its capabilities to train machine learning models using cloud-based datasets. This cloud-based approach not only streamlines the model creation process but also opens the door to enhanced scalability and efficiency in handling large and diverse datasets. As we delve deeper into the experiment, we will unveil the precise ways in which Azure Web Services were employed to optimize the prediction model and catalyze the automation of the detection process, ultimately leading to expedited results with superior accuracy.

3.2 Comparing Algorithm Features

Table 2 presents a comprehensive comparison of various algorithms, highlighting both their distinct advantages and limitations. This table serves as a valuable reference for evaluating the suitability of different techniques for specific applications

Table 2: Advantages and Limitations of Common Machine Learning Algorithms

Algorithm	***Learning Method***	***Advantage***	***Limitation***
Linear Regression	Supervised	Simple and computationally efficient, easy to interpret the results	Assumes a linear relationship between the dependent and independent variables
Logistic Regression	Supervised	Can model non-linear decision boundaries and provide probabilistic output	Can be sensitive to overfitting and the choice of regularization parameter
Decision Trees	Supervised	Easy to interpret and visualize, can handle both numerical and categorical data	Can be prone to overfitting and can be sensitive to the choice of hyperparameters
Support Vector Machines (SVM)	Supervised	Can effectively model non-linear decision boundaries in high-dimensional spaces	Can be sensitive to the choice of kernel function and parameters
K-Nearest Neighbors (KNN)	Supervised	Can easily adapt to new data and can be effective for classification tasks with a small number of classes	Can be computationally expensive for large datasets and can be sensitive to the choice of distance metric
Naive Bayes	Supervised	Can be trained with small amounts of data and is computationally efficient	Assumes independence between the predictor variables
Artificial Neural Networks (ANN)	Supervised	Can effectively model highly complex patterns and relationships in data	Requires a large amount of data to train effectively and can be computationally expensive to

			train and deploy
Convolutional Neural Networks (CNN)	Supervised	Ability to automatically learn and represent highly complex patterns and relationships in image and video data	Requires a large amount of data to train effectively and can be computationally expensive to train and deploy
Recurrent Neural Networks (RNN)	Supervised	Can effectively model sequential data such as time series and natural language	Can suffer from vanishing or exploding gradients during training
Long Short-Term Memory (LSTM)	Supervised	Can effectively model long-term dependencies in sequential data	Can be computationally expensive to train and deploy
K-Means	Unsupervised	Simple and computationally efficient, easy to interpret and visualize	Requires the choice of the number of clusters and can be sensitive to the choice of initialization of cluster centroids
Multiclass Neural Network	Supervised	Can handle multiple classes	Requires a large amount of labeled data for training
Multiclass Regression	Supervised	Can handle continuous and categorical inputs	Assumes a linear relationship between inputs and outputs
Two Class Locally Deep Support Vector	Supervised	Nonlinear decision boundary	Computationally intensive with large datasets

The choice of algorithm in our study was based on the nature of the challenge, the available data, and the desired outcomes. We chose multiclass neural network [38] because it is capable of handling multiple classes and can learn complex relationships between inputs and outputs. Multi-class regression, on the other hand, can handle both continuous and categorical inputs, making it suitable for problems with mixed data types. Finally, the two-class locally deep support vector can capture nonlinear decision boundaries and may perform better than other linear algorithms in such cases.

3.3 Manual Feeding vs Automatic Feeding

Figure 1 vividly depicts the diagram pivotal to this study's methodology. At its core, it delineates the two distinct feeding processes employed: the manual feeding process and the automatic feeding process.

In the manual feeding process, the foundation for model construction is established upon an existing dataset that was carefully curated and introduced for this purpose. This dataset serves as the bedrock upon which the model is built, providing historical information and patterns crucial for its training and development.

Conversely, the automatic feeding process represents a dynamic approach that ushers in real-time data from the IPS/IDS (Intrusion Prevention System/Intrusion Detection System) model. This real-time data is seamlessly integrated with the pre-existing dataset, imbuing it with the most current and up-to-the-minute information. This amalgamated dataset is then channeled into the subsequent phases of model building, infusing the model with the agility and responsiveness needed to adapt to evolving threats and circumstances.

In essence, Figure 1 encapsulates the pivotal role of these two feeding processes in shaping the experiment's methodology, highlighting the transition from historical data reliance to a real-time, adaptive model construction approach.

3.4 Metrics Used

To effectively harness the capabilities and to exploit the metrics of azure machine studio, and compare the collected results of each algorithm used, we need to identify the derived metrics from each classification model [39]. The following key metrics are the major metrics used to measure anomalies traffic in a network:

True Positive (TP): Where a model predicts a result in the class positively correct.
True Negative (TN): Similar to the true positive, where a model predicts a result in the class negatively correct.

False Positive (FP): Where a model predicts a result in the class positively incorrect
False Negative (FN): Where a model predicts a result in the class negatively incorrect

Given the four criteria of the network traffic, we then derive the following metrics:

3.4.1 Accuracy

Accuracy is one of the critical factors used to measure the performance of a model, particularly in classification tasks. It provides an overall assessment of how well a model is performing by measuring the ratio of correctly predicted instances to the total instances evaluated. It is calculated using the following formula:

$$Accuracy = \frac{(TP+TN)}{\sum(TP+TN+FP+FN)} \quad [32]$$

3.4.2 Precision

The precision is a metric that ranges between 0 and 1, and it measures the accuracy of positive predictions made by a classification model and it is calculated as follows:

$$Precision = \frac{TP}{(TP+FP)} \quad [33]$$

3.4.3 Recall

The recall is the total true positives divided by the total of true positive and false negative. It is helpful in assessing performance.

$$Recall = \frac{TP}{(TP+FN)} \quad [34]$$

3.4.4 Error rate

The difference in percent value from the collected results versus the actual value is divided by the actual value.

$$Error\ rate = \frac{|Observed\ Value - Actual\ Value|}{Actual\ Value} * 100 \quad [35]$$

3.4.5 F-Measure

The F-measure is also called the F1 score and it is calculated as follows:

$$F - measure = \frac{(2*Precision*Recall)}{(Precision+Recall)} \quad [36]$$

3. EXPERIMENTS AND RESULTS DISCUSSION

The feeding of the CSE-CIC-IDS2018 to our model to train can be done manually or automatically. Manual feeding involves manually selecting and inputting the data into the algorithm, whereas automatic feeding uses an automated tool to retrieve and input the data. In this section, we will compare the previously introduced metrics to gauge the performance of each experiment.

Figure 2. shows the statistics collected from this experiment.

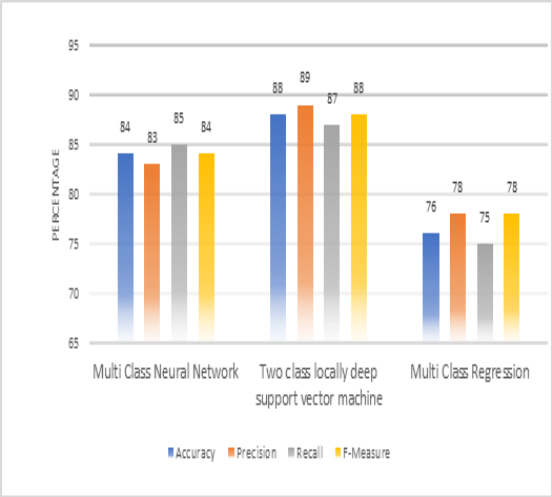

Figure. 2 Graph of the performance of three used algorithms before using the automatic feeding

In the performed experiment using multiclass neural network, multiclass regression, and two-class locally deep support vector machine in Azure Machine Learning Studio, the two-class locally deep support vector machine achieved the highest accuracy of 88%, precision of 89%, recall of 87%, and F-measure score of 88%. The multiclass regression algorithm achieved an accuracy of 76% with a precision of 78%, recall of 75%, and F-measure score of 78%. The multi-class neural network algorithm achieved an accuracy of 84% with a precision of 83%, recall of 85%, and F-measure score of 84%.

Since further optimization and testing are necessary to get better metrics, we performed the second experiment using the automatic feeding

through the Azure Web Services feature and Figure 3. Shows the found results.

Figure. 3 Graph of the performance of three used algorithms after using the automatic feeding

Table 3 presents a detailed comparison of the performance achieved in two experiments, highlighting the percentage difference between the results. It provides a comprehensive overview of the key metrics measured, such as accuracy, precision, recall, and F-measure score, and demonstrates how these measures differ between the two experiments. Importantly, the second experiment outperformed the first one across all key metrics, with a significantly higher percentage difference for each measure. This improvement can be attributed to the use of the automatic feeding method through Azure web services, which provided automation and efficiency that was lacking in the first experiment's manual approach. The integration of Azure web services proved to be a highly effective strategy for optimizing performance and achieving better results.

Table 3: Percentage Difference in Metrics Between the Experiments

Metric	*Multi Class Neural Network*	*Two Class Locally Deep Support Vector Machine*	*Multi Class Regression*
Accuracy	*7.1%*	*10.2%*	*5.3%*
Precision	*6.0%*	*6.7%*	*5.1%*
Recall	*5.9%*	*8.0%*	*5.3%*
F-Measure	*4.8%*	*5.7%*	*3.8%*

Based on these results, the two-class locally deep support vector machine performed the best on this particular case, but the other algorithms also achieved reasonably good results. The two-class locally deep support vector machine obtained the highest accuracy of 97% and had a precision of 95%, recall of 94%, and F-measure score of 93%. In comparison, the multiclass regression algorithm had an accuracy of 80%, a precision of 82%, a recall of 79%, and an F-measure score of 81%. On the other hand, the multi class neural network algorithm achieved an accuracy of 90%, a precision of 88%, a recall of 90%, and an F-measure score of 88%.

By leveraging automatic feeding through Azure web services, we were able to achieve the highest level of performance compared to manual feeding. The automation allowed for more efficient and accurate data processing, which led to improved results. Consequently, the integration of automatic feeding through Azure web services proved to be a highly effective strategy for optimizing the detection rate. Table III shows a comparison of the performance between the two experiments and calculates the percentage difference.

4. CONCLUSION AND FUTURE WORK

In conclusion, as the landscape of cyber threats continues to evolve with increasing complexity, the integration of various machine learning algorithms within cloud-based platforms emerges as a pivotal safeguard for fortifying the security of both systems and data. Among the arsenal of tools available, web service portals stand out as potent instruments for bolstering cloud security, with a promising trajectory of adoption in the years ahead. This article has elucidated the potent capabilities of Azure Machine Learning Studio's web service portal, showcasing how it can be harnessed to augment the real-time performance of trained models. By harnessing insights derived from network packet behavior analysis, this methodology enhances detection accuracy and empowers organizations to respond swiftly to emerging threats. Looking forward, the horizon of research is poised to focus on the development of an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) capable of learning dynamically from real-time network packet behavior. This innovative approach aims to construct a seamless mechanism for transferring packet attributes to a web server housing the model, thus facilitating continuous real-time learning for the IDS. Ultimately, this endeavor will contribute significantly to the creation of a robust knowledge base for threat detection and mitigation within IDS and IPS systems.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] Wadiai, Younes, and Mohamed Baslam. "Machine Learning Approach to Automate Decision Support on Information System Attacks." International Conference on Business Intelligence. Springer, Cham, 2022.

[2] Zuech, Richard, John Hancock, and Taghi M. Khoshgoftaar. "Detecting web attacks using random undersampling and ensemble learners." Journal of Big Data 8.1 (2021): 1-20.

[3] Khan, Muhammad Ashfaq, and Juntae Kim. "Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset." Electronics 9.11 (2020): 1771.

[4] ÇİMEN, Fethi Mustafa, Y. U. S. U. F. Sönmez, and M. U. S. T. A. F. A. İlbaş. "Performance Analysis of Machine Learning Algorithms in Intrusion Detection Systems." Düzce Üniversitesi Bilim ve Teknoloji Dergisi 9.6 (2021): 251-258.

[5] Kanimozhi, V., and T. Prem Jacob. "Calibration of various optimized machine learning classifiers in network intrusion detection system on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing." International Journal of Engineering Applied Sciences and Technology 4.6 (2019): 2455-2143.

[6] Aljamal, Ibraheem, et al. "Hybrid intrusion detection system using machine learning techniques in cloud computing environments." 2019 IEEE 17th international conference on software engineering research, management, and applications (SERA). IEEE, 2019.

[7] Maheswari, K. G., C. Siva, and G. Nalini Priya. "An Optimal Cluster Based Intrusion Detection System for Defence Against Attack in Web and Cloud Computing Environments." Wireless Personal Communications (2022): 1-27.

[8] Butt, Umer Ahmed, et al. "A review of machine learning algorithms for cloud computing security." Electronics 9.9 (2020): 1379.

[9] Jairu, Pankaj, and Akalanka B. Mailewa. "Network Anomaly Uncovering on CICIDS-2017 Dataset: A Supervised Artificial Intelligence Approach."

[10] Qaddoori, S. L., & Ali, Q. I. (2021). AN IN-DEPTH CHARACTERIZATION OF INTRUSION DETECTION SYSTEMS (IDS). Journal of Modern Technology and Engineering, 6(2), 161-188.

[11] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[12] Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. Applied Sciences, 12(22), 11752.

[13] Ndibwile, J. D., Govardhan, A., Okada, K., & Kadobayashi, Y. (2015, July). Web server protection against application layer DDoS attacks using machine learning and traffic authentication. In 2015 ieee 39th annual computer software and applications conference (Vol. 3, pp. 261-267). IEEE.

[14] Jayalaxmi, P., Saha, R., Kumar, G., Conti, M., & Kim, T. H. (2022). Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey. IEEE Access.

[15] Uğurlu, M., Doğru, İ. A., & Arslan, R. S. (2021). A new classification method for encrypted internet traffic using machine learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2450-2468.

[16] Garcia, J. F. C., & Blandon, G. E. T. (2022). A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks. IEEE Access, 10, 83043-83060.

[17] Singh, L., & Jahankhani, H. (2021). An Approach of Applying, Adapting Machine Learning into the IDS and IPS Component to Improve Its Effectiveness and Its Efficiency. Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges, 43-71.

[18] Amrollahi, M., Hadayeghparast, S., Karimipour, H., Derakhshan, F., & Srivastava, G. (2020). Enhancing network security via machine learning: opportunities and challenges. Handbook of big data privacy, 165-189.

[19] Bains, J. S., Kopanati, H. V., Goyal, R., Savaram, B. K., & Butakov, S. (2021, November). Using Machine Learning for malware traffic prediction in IoT networks. In 2021 Second International Conference on

Intelligent Data Science Technologies and Applications (IDSTA) (pp. 146-149). IEEE.

[20] Karatay, M., & Emirtekin, E. (2021). MACHINE LEARNING APPLICATIONS FOR ANOMALY DETECTION. INFORMATION SECURITY: PROBLEMS AND PROSPECTS, 66.

[21] Sokolov, S. A., Iliev, T. B., & Stoyanov, I. S. (2019, May). Analysis of cybersecurity threats in cloud applications using deep learning techniques. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 441-446). IEEE.

[22] Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Koyuncu, M. (2022). Cybersecurity deep: approaches, attacks dataset, and comparative study. Applied Artificial Intelligence, 36(1), 2055399.

[23] Ali, R., Ali, A., Iqbal, F., Hussain, M., & Ullah, F. (2022). Deep Learning Methods for Malware and Intrusion Detection: A Systematic Literature Review. Security and Communication Networks, 2022.

[24] Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. (2022). Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions. Security and Communication Networks, 2022.

[25] Agarwal, A., Khari, M., & Singh, R. (2021). Detection of DDOS attack using deep learning model in cloud storage application. Wireless Personal Communications, 1-21.

[26] Ahmet, E. F. E., & ABACI, İ. N. (2022). Comparison of the Host Based Intrusion Detection Systems and Network Based Intrusion Detection Systems. Celal Bayar University Journal of Science, 18(1), 23-32.

[27] Catillo, M., Rak, M., & Villano, U. (2019). Discovery of DoS attacks by the ZED-IDS anomaly detector. Journal of High Speed Networks, 25(4), 349-365.

[28] Mighan, S. N., & Kahani, M. (2021). A novel scalable intrusion detection system based on deep learning. International Journal of Information Security, 20, 387-403.

[29] Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing, 1-37.

[30] Ayo, F. E., Folorunso, S. O., Abayomi-Alli, A. A., Adekunle, A. O., & Awotunde, J. B. (2020). Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. Information Security Journal: A Global Perspective, 29(6), 267-283.

[31] Bolatti, D. A., Todt, C., Scappini, R., & Gramajo, S. (2022, August). Network traffic monitor for ids in iot. In Cloud Computing, Big Data & Emerging Topics: 10th Conference, JCC-BD&ET 2022, La Plata, Argentina, June 28–30, 2022, Proceedings (pp. 43-57). Cham: Springer International Publishing.

[32] Walther, B. A., & Moore, J. L. (2005). The concepts of bias, precision and accuracy, and their use in testing the performance of species richness estimators, with a literature review of estimator performance. Ecography, 28(6), 815-829.

[33] Martel, M. (2009, January). Program transformation for numerical precision. In Proceedings of the 2009 ACM SIGPLAN workshop on Partial evaluation and program manipulation (pp. 101-110).

[34] Davis, J., & Goadrich, M. (2006, June). The relationship between Precision-Recall and ROC curves. In Proceedings of the 23rd international conference on Machine learning (pp. 233-240).

[35] Gijsberts, A., Atzori, M., Castellini, C., Müller, H., & Caputo, B. (2014). Movement error rate for evaluation of machine learning methods for sEMG-based hand movement classification. IEEE transactions on neural systems and rehabilitation engineering, 22(4), 735-744.

[36] García, S., Fernández, A., Luengo, J., & Herrera, F. (2009). A study of statistical techniques and performance measures for genetics-based machine learning: accuracy and interpretability. Soft Computing, 13, 959-977.

[37] Diaz-Vico, D., Prada, J., Omari, A., & Dorronsoro, J. (2020). Deep support vector neural networks. Integrated Computer-Aided Engineering, 27(4), 389-402. Martineau, M., Raveaux, R., Conte, D., & Venturini, G. (2020). Learning error-correcting graph matching with a multiclass neural network. Pattern Recognition Letters, 134, 68-76.

[38] Gasso, G. (2019). Logistic regression. INSA Rouen-ASI Departement Laboratory: Saint-Etienne-du-Rouvray, France, 1-30.

[39] Mughaid, A., AlZu'bi, S., Alnajjar, A., AbuElsoud, E., Salhi, S. E., Igried, B., &

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Abualigah, L. (2022). Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches. Multimedia Tools and Applications, 1-23.

[40] Joshi, H., & Patel, B. K. (2012, August). Towards application classification with vulnerability signatures for IDS/IPS. In Proceedings of the First International Conference on Security of Internet of Things (pp. 216-221).

Journal of Theoretical and Applied Information Technology
30th November 2023. Vol.101. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

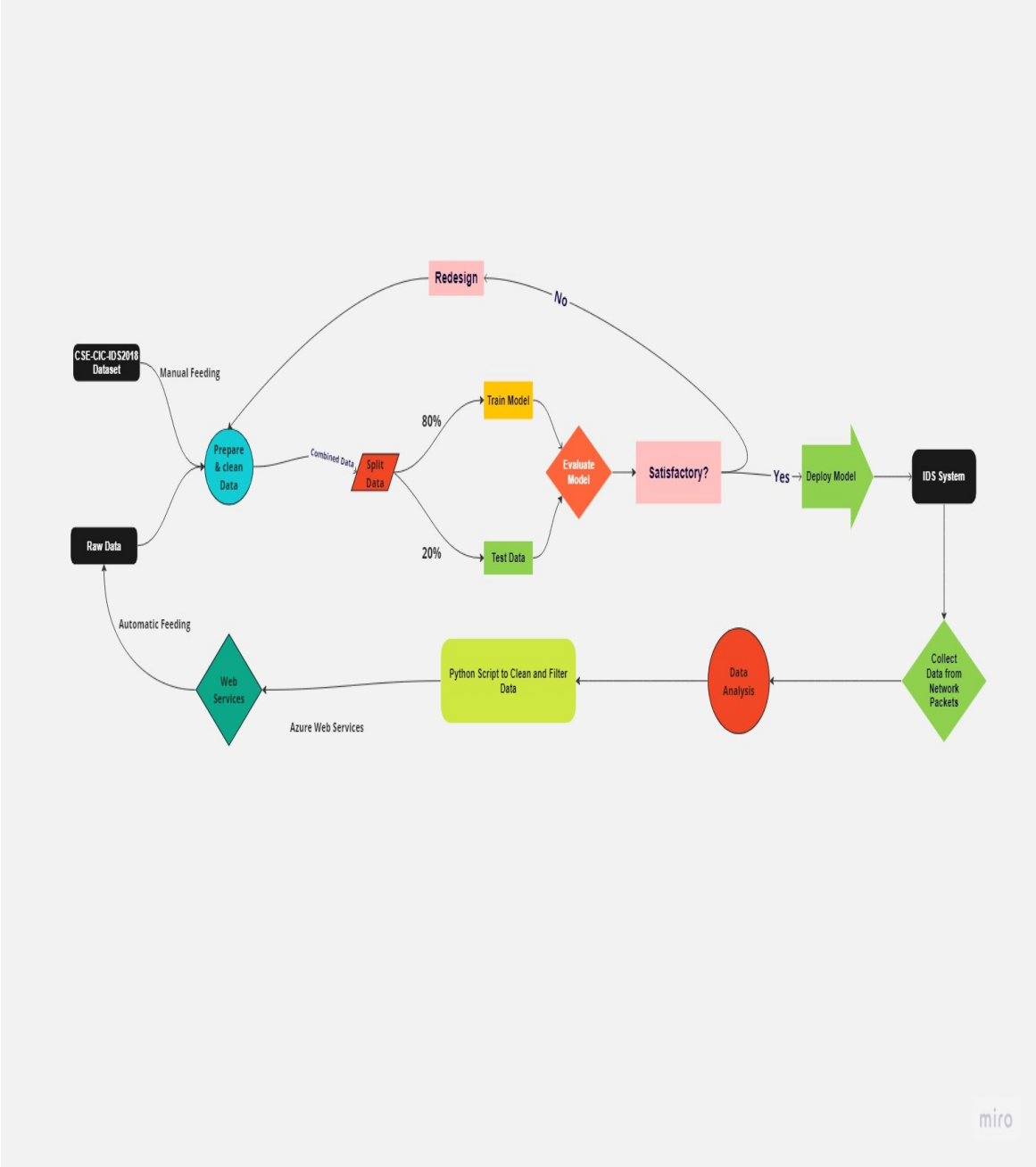

Figure. 1 Flow chart of the proposed model