Performance Comparison of various Machine Learning & Deep Learning Algorithms for Intrusion Detection Systems

By Vijay Tyagi

Thesis Supervisor
Dr Kiran Kumar V G

Table of Contents

1. Background

McAfee report says cybercrime to cost world economy over $1 trillion

(McAfee Report Says Cybercrime to Cost World Economy over $1 Trillion | Business Standard News, n.d.)

Impact of cyber-attack on the organization business: All cyber-attack creates big impact to the organizations business, it affects organizations revenue stream, as well as the customers loose trust in the business.

Primary the effect of security breach can be classified into 3 categories:

1. Financial Loss to the Organization
2. Reputational Loss to the Organization
3. Legal Issue faced by the Organizations

Financial Loss due to the cyber attack

Cyber-attacks mainly lead to a significant financial loss because of:

Attackers steal organization business critical data. Attackers steal organization financial information which can have data related to their Bank accounts & Payment related details too. The Attacker directly steal the money of organization accounts by stealing their bank accounts details & conducting the wire transfer of the money. The Attacker disturb the business operation my create disturbance in organizations business critical applications of process. When organization business critical application or process is not operational then it can lead to the revenue loss to the organization & also their entire workforce productivity goes down. Business also gets major financial loss as they have to restore their operations which is a very taxing process as lot of money is incurred in it.

Reputational Loss to the Organization

The entire building block on any business is based on the customer's trust

Every cyber-attack shakes the trust of the customers as their confidence level goes down, because if any organization is not able to secure their own data how come they can secure customer data & their infrastructure. Which negatively impact the business due to Organization loses the customer, Organization sales gets impacted as they don't have the customers to buy their solutions. Since Organizations are not able to sell anything, automatically it leads to the revenue loss & also the employee start leaving the organizations

Legal Issue faced by the Organizations

Now a days the Data protection and privacy laws are very stringent & they require organizations to not only secure their data but the data of their customers also

Personal data laws like GDPR can impose huge penalty loss to the organization if they found that the organization has not followed due care & due diligence to secure the PII (Personal Identifiable Information) of the employees, similarly every other county in the world has very stringent laws & regulations to protect the data (*Impact of Cyber Attack on Your Business | Nibusinessinfo.Co.Uk*, n.d.)

2. Problem Statement

It is observed from the review of related research that Cyber-attacks are now a major source of concern for all enterprises throughout the world. Hence the significant problem would be to build a network intrusion detector system based preventive model which will be capable to differentiate between a genuine connection or good connection & attacker connection or bad connection. Now a days cyber-attacks are main problematic areas of all organizations across the world

Network Based Intrusion Detection System (NIDS), or Network Based IDS, is security solution that is placed to monitor critical network traffic. Newer IDS solutions use Machine Learning to access the network traffic for patterns of interest (attacks). When IDS detect a pattern of traffic which it classifies as network-based attack then typically it sends the alert to the Security Operation Team, who investigate that incident to detect any possibility of attack. Intrusion Detection System (IDS) is a software-based solution which run on top of a hardware appliance to detect network-based intrusion using different machine learning algorithms. IDS monitors are placed across the strategic locations withing the network to protect the organization infrastructure from any intrusion activity & mitigate the malicious threat actor to infiltrate the organization infrastructure. The ML based IDS is programmed to build a predictive model which can distinguishing between bad connections and a good connection.

Intrusion Detection System are helpful for the organizations to:

- Detect the incoming and outgoing network-based traffic.
- It also detects the malicious traffic patterns or abnormalities in the network traffic continuously.
- It immediately triggers an alarm once it detects any intrusion activity or any threat actor try to infiltrate the organization network Infrastructure.

Various form of Intrusion Detection Systems is listed below in today’s security environment

Host Based Intrusion-Detection System (HIDS)

Company uses a Host based Intrusion Detection System on the end user Laptop or Desktop machines. The, HIDS continuously monitor the traffic which is coming in & going out on the individual machines, whenever it detects any malicious patter or behaviours in the network traffic it immediately sends an alert to the security team of the organization

HIDS primary work on the predefined signatures which get continuously updated by the HIDS solution vendor, whenever it detects any traffic pattern matching the signatures it immediately generates an alert

Protocol-based IDS (PIDS) Systems

Company uses PIDS in front of their critical servers which are hosting the business-critical applications. it examines the communication of protocols between the server and the end user. It also monitors the HTTPS & HTTP based traffic to secure the web-based traffic.

Whenever it sees any malicious pattern the in web-based traffic, it immediately generates the alert.

Hybrid Intrusion Detection System (HIDS)

HIDS is a combination of two different solutions, they are developed which the functionality of Host based Intrusion Detection Systems & Network based Intrusion Detection Systems, Overall, their efficacy is good as they mitigate the malicious traffic at two different layers of the network architecture

Protocol-based IDS (PIDS)

Company uses PIDS in front-end of their critical servers or applications.

PIDS continuously check the traffic between the server and end user which is initiating the connection, PIDS inspect the HTTP or HTTPS based web server, Similarly, we can have PIDS for different protocol also like for Domain Name Server (DNS) traffic, File transfer Protocol (FTP) traffic, Mail traffic etc. We can see that the newer intrusion techniques and malware are increasing gaining the momentum significantly and attackers are using newer methodology to infiltrate the organizations network. Hackers use new methods to infiltrate organization Infrastructure so for such kind of malicious activates we need to have newer methodology to detect the sophisticated attacks. Now a days the security team primarily uses Machine learning to create a machine learning model. If in case the existing signature-based IDS is not able to detect any malicious traffic or attack pattern then the ML based detection model identify the attack, basically it uses any anomaly in the traffic pattern. Overall, it has been observed that the anomaly-based Intrusion Detection Systems are more efficient in comparison to the legacy signature-based IDS solutions

Hybrid Detection Method (HDM)

A Hybrid IDS utilize both Signature database and Anomaly-based intrusion detection methods together. As its evident that the attacks are becoming more sophisticated, hence we need newer ways to mitigate them also (*Intrusion Detection System (IDS) - GeeksforGeeks*, n.d.)

The different types of Network attacks which are largely prevalent now a days are listed below:

Scanning Attacks

In this kind of network attack the attacker use the network scanning techniques, they send the PING packet of large group of IP Addresses, in order to detect which machines are operational on the Internet, Once the attacker detects the Live machine then they further scan those machines to detect which Port & Protocol are open on that machine

They also check the Operating Systems those machines are using, as they us ethe vulnerabilities in those Operating Systems to infiltrate those machines

SQL injection attacks

Once the attacked detect that the SQL is running on the machine after using their scanning techniques, they try to use various attack on the SQL OS because SQL has lot of inherent vulnerabilities in itself

Asymmetric Routing

Asymmetric routing is when the intended traffic is routed somewhere else spite of their intended destination, which can crease loops in the traffic & the attacker get hold of the traffic

Man in Middle Attack

In this kind of network attack the attacker try to present himself as a genuine user & try to steal the credential or critical information of the genuine user

For example, if the organization use is trying to access their corporate emails, then the attacker tries to present himself as the Organization email server & try to capture the organization use email credentials, which they use to initiate more attacks to the other employee of the same organization

Buffer Overflow Attacks

In this type of cyber-attacks, the attack tries to over consume the CPU & memory of the target systems, it replaces the normal data with bogus data, which they send frequently, as a result the target machine all hardware resources got consumed to respond back on the bogus attacker traffic which leads to the crash of the operating systems running on the target machines

Protocol-Specific Attacks

These kinds of attacks are targeted to the specialized protocols, like ARP, ICMP & TCP traffic. **ICMP** means Internet Control Message Protocol and it is consumed by the infrastructure devices to pass the communication message with each other. The ping and traceroute are the utilities which are used by the ICMP for communications. The ICMP attacks are also called as Ping sweeps, in this the attacker continuously send ICMP echo-request packet to the target systems so its all resources got consumed to respond on these bogus packets, as a result the device is not able to respond back on the genuine requests and crashed down**.** The attacker also uses heavy packet size in the ICM request so the target system consumes also its resources to respond on the attacker ICMP request

ARP means Address Resolution Protocol, and used by the attackers, attacker send many ARP packets to the target machine, as a result the target machine consumes all its resources to respond back on those bogus packets & ultimately the target system gets crashed

The attacker can also respond back with its our ARP response MAC address so the genuine user gets confused & initiate the TCP connection with the attacker machine, which leads to the compromise of the Organizations user traffic, this type of attack is also called as ARP poisoning attack

Malware

In today's network environment we can observer various kind of malwares, which include bots, ransomware, Viruses and trojan horses. Malware compromises of a software-based entity which is created to damage or corrupt the target systems.

Now a days the major source of malware spread is through emails, in which the Organization user by mistake download the email attachment which are infected with various malware

The malware also tries to attack the inherent vulnerabilities in the target machine

The major types of malwares are *worms and viruses*.

These malwares can attach themselves to a genuine file or document and spread quickly throughout the organization network system.

Worms can independently transfer from one machine to another withing the organization, whereas the Virus need any host to transfer them from one machine to the another one

A trojan horse file can hide itself in as a normal genuine software-based program, such as a file or the document looks legitimate but it is infected by the malware.

The worms can replicate themselves, whereas the virus need some transport mechanism to propagate themselves. The Bots can replicate to a genuine file or device and then they connect back to their central command & control server.

Traffic Flooding

This kind of cyber-attack are also called as a Distributed Denial of Service attack.

In this the attacker filled the hardware & software resource of a system with bogus packet request so that the system become unresponsive(*10 Types of Cyber Attacks You Should Be Aware in [2021]*, n.d.)

Various research is carried in this regard and analysis of some of them are:

1. Gupta detected the network attacks on the IoT infrastructure, their proposed DLHNN classifier were able to attains 99.52% classification accuracy (Gupta et al., 2022)
2. Campose et el simulated the IoT traffic and applied the Federated Learning methodology to check the efficacy of IDS solution,
   For future work they want to test the algorithm on the live IoT traffic (Campos et al., 2022)
3. Saveetha & Maragatham used Block Chain based IDS by using Deep Learning algorithm , they found that Block chain has a major role in the IDS based solutions (Saveetha & Maragatham, 2022)
4. M.P studied the IDS using Big data & Hadoop Database , they were able to achieve the maximum precision of 0.8800, maximum recall of 0.8845, and maximum F-measure of 0.8822In future they want to use different DL algorithms to enhance the efficacy further (M .P . et al., 2022)
5. Kumar researched the IOT network along with Blockchain, they proposed a model of IDS for IOT and FOG computing ,As per the future plans they want to extend this work by applying different deep learning techniques, to improve IDS detection rate (Kumar et al., 2022)
6. Kilincer et al created a new IDS dataset and used boosting algorithms to detect the efficacy of the IDS system ,They identified that the LGBM and XGBoost classifiers have higher efficacy rate in comparison to other classifiers For future work they want to work on the live IoT based network and check the efficacy of their model (Kilincer et al., 2022)
7. Samriya et al utilize the cloud base infrastructure to check the efficacy of ML based IDS model ,In this research they use a novel ACO-DNN hybrid classifier model (Samriya et al., 2022)
8. Baldini & Amerini proposes an online algorithm based on a sliding window with the novel application of the Morphological Fractal Dimension (MFD) to the network intrusion problem , they found it enhance the IDS model performance (Baldini & Amerini, 2022)
9. Guarascio et al studied ORISHA which is a first attempt to enable a sharing and interoperability protocol among such components, based solely on a data-oriented approach. Their study helps in detection of undetected attacks also (Guarascio et al., 2022)
10. Bangui & Buhnova studied Mobile Edge Computing infrastructure to build the IDS model They used and Deep Forest algorithms to support the reliability of lightweight IDSs for highly distributed MEC environments. As a future work they want to experiments with more bio-inspired algorithms to check the IDS model efficacy (Bangui & Buhnova, 2022)

3. Aim and Objectives

The main aim of this research is to propose a precious Intrusion detection rate on the Network dataset using various Machine Learning & Deep learning algorithms.

The research objectives are formulated based on the aim of this study which are as follows:

In this proposal various Machine Learning algorithms & Deep Learning algorithm to check the Intrusion attempt on the dataset & check they efficacy. This study will have a significant value for the cyber security field, as current IDS software is typically able to recognize the Intrusion attempts using signature-based solution or anomaly-based detection, using Machine Learning & Deep Learning will have significantly higher accuracy intrusion detection rates. Machine Learning & Deep Learning plays a very instrumental role in the automation of attacks detections.

4. Significance of the Study

What impact this study is that the network-based intrusion can collapse the business one entire organization across the globe, hacking & DDOS is improving day by day & its essential to have updated knowledge to mitigate any contiguous approach.

So, this study will help in the creating better approach in the mitigation of cyber-attacks & checking the efficacy of various ML & DL algorithms

5. Scope of the Study

The scope is limited to evaluate various Machine Learning and Deep Learning algorithms and check their efficacy comparison on the dataset

6. Research Methodology

This research Methodology have processes such as the to select the relevant dataset, modify the the data into a structured and readable format, using the data balancing techniques, incorporate the supervised learning techniques and checking the machine learning performance using various evaluation criteria's.

Brief Introduction of various Machine Learning Algorithms

Basics of Machine Learning

Artificial Intelligence is an umbrella term and it has many sub parts in which Machine Learning is one of its parts.ML articulate as how a machine can respond on a question or how it can make a decision by using its various algorithms.

It differentiates from the legacy programming software approach, as they require to defined the set codes as well as the instruction and the software behave based on the pre-defined instructions

We have primary three kind of Machine Learning Algorithms

1. Supervised learning
2. Unsupervised learning
3. Deep learning or Neural Networks

Supervised Learning

In case of the supervised learning, the computer is taught using the sample of data that is classified to instruct the machine what the data actually represents.

Unsupervised Learning

In case of unsupervised learning, the machine is taught by utilizing the data that doesn't have any labels. This mean the machine doesn’t have an understanding of the data type neither it is aware what to expect out of that data. The machine itself have to understand the various pattern in the data and come to the conclusion of the desired results also

Deep Learning

Deep Learning is a specialised methodology of machine learning architecture which utilize humans like artificial neurons at different interconnected layers to understand the given data. Deep learning is primarily very much instrumental which we are trying to learn the various data pattern from an unstructured data set

Main Machine Learning Algorithms

1. Random Forest (RM)
2. K-Means
3. K-Nearest Neighbour (KNN)
4. Support Vector Machine (SVM)
5. Decision Tree (DT)
6. Naive Bayes (NB)
7. Linear Regression (LR)
8. Logistic Regression (LR)

1. **Random forest** This algorithm is part of Supervised Machine Learning Algorithm which is mainly utilize in the Classification and Regression related problems. It constructs a decision tree by using various different samples and make their majority sample for classification and also average them in case of regression algorithms
2. **k- Nearest Neighbor (KNN)** This algorithm can be utilised for both the classification and regression problems. But primarily it is used in classification problems in the industry.
3. **Support Vector Machine (SVM)** In this type of method we do the sorting of the data, we draw each data item as a point in n-dimensional space into the value of each feature being the value of the particular coordinate.
4. **Decision Tree** This algorithm categorizes into the supervised learning algorithm which is used for classification related problems. In this type of algorithm, we split the data in 2 or more similar kind of sets. This is achieved based on significant attributes or independent variables to make as distinct groups as possible.

5. **Naive Bayes** It is a differentiation technique which is based on the Bayes' theorem with an assumption of no relation between the predictor's values
6. **K-Means** This algorithm is part of unsupervised algorithm which help in the clustering-based problems
7. **Linear Regression** It is used to give an estimation of real values (example could be the prediction of house prices, total call a call centre will receive, what should be the marketing budget to get an approximate business etc.) based on the values of continuous variables. Here we try to create a link between the independent variable and the dependent variables by placing the data into a best line.
   The best fit line is called as the regression line and it is represented by the linear equation Y= a *X + b.
8. **Logistic Regression** Logistic regression is one of the important ML algorithms, which are part of Supervised Learning technique. It is used to predict the categorical dependent variable using a given set of independent variables. (*Commonly Used Machine Learning Algorithms | Data Science*, n.d.)

What is Deep Learning or Neural Network:

A neural network or the Deep Learning (Figure-1) is structured which resembles the human like brain and like human neurons it is made up of artificial neurons, also known as nodes in the algorithm.

These nodes are combined with each other in three-layer architecture:

1. The input Layer
2. The hidden Layer
3. The output Layer

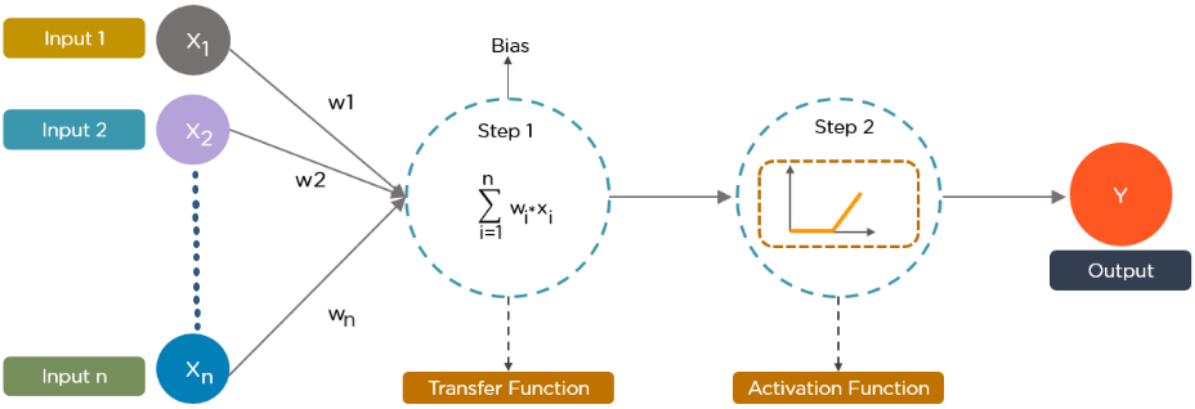


Figure-1: How Deep Learning or Neural Network Works

Deep Learning or Neural Network Algorithms

1. Recurrent Neural Networks (RNNs)
2. Long Short-Term Memory Networks (LSTMs)
3. Convolutional Neural Networks (CNNs)

Recurrent Neural Networks (RNNs)
This algorithm has connection that can form the guided patterns, which create the outputs from the LSTM which is goes as the inputs to the current phase of the cycle.

Long Short-Term Memory Networks (LSTMs)
LSTMs are the part of RNN's that can learn and memorize long-term interdependencies.
It memorizes the past based information for long periods is its key behaviour.

Convolutional Neural Networks (CNNs)
CNN is also known as Convents', which is made up of multiple layers and are primarily utilize for the image processing and object detection. (*Top 10 Deep Learning Algorithms You Should Know in 2022*, n.d.)

<u>My Approach is as following:</u>

First step will be to choose the right Dataset, Supervised ML & DL needs some data to train & learn.ML & DL algorithm require lot of data along with the relevant one
In my study I will use the data sets from the following locations:

Dataset Link

http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

This is the data set which was utilized in the 3rd International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99
The Fifth International Conference on Knowledge Discovery and Data Mining.

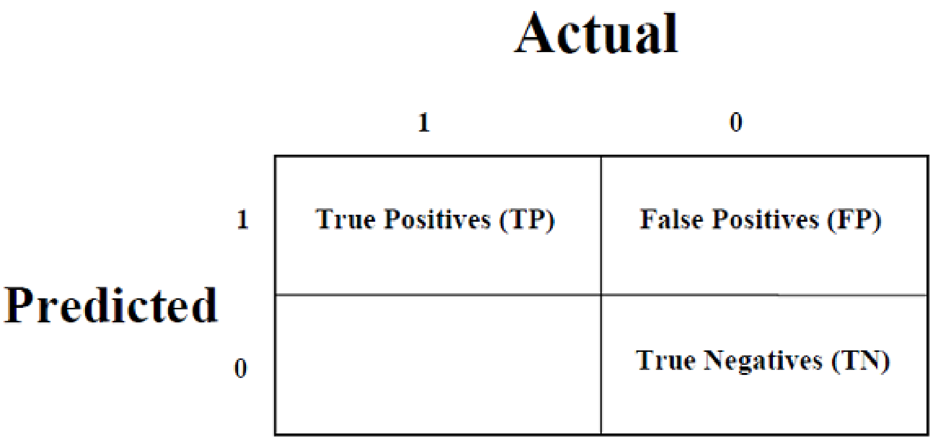
In this study the various Network based cyber-attacks will be categorized as :

- Denial-of-service attack, an example will be the sync flood attack
- An attacker trying to access the target machine by unauthorized means from a remote location an example will be the password breaking attack
- The attacker is trying to access the machine administrative account by unauthorized way, an example will be the Buffer overflow attacks

- Sniffing or probing, in which the attacker if trying to steal the information through various social engineering & surveillance methodology,
- an example will be the port scanning using ICMP protocol

Second step will be to clean the data set & remove unnecessary fields
Third step will be to apply the various ML and Deep Learning Algorithms on the dataset like: Linear Regression, Logistic Regression, Decision Tree, Naive Bayes, kNN, K-Means and the Random Forest As well as the Deep Learning algorithms like:
Convolutional Neural Networks (CNNs), Long Short-Term Memory Networks (LSTMs) and the Recurrent Neural Networks (RNNs)
Fourth step will be to compare their results of various algorithms applied and compare their efficacy rate

Following Performance Metrics are used for the Classification Problems of ML & D
Confusion Matrix (*Figure-2)*
It is the procedure to measure the functioning of a classification problem when the output can be of different classes type.



		Actual	
		1	0
Predicted	1	True Positives (TP)	False Positives (FP)
	0		True Negatives (TN)

Figure-2: Confusion Matrix terminology

The terms associated with the confusion matrix are depicted in the Table-1 and Table-2:
Table-1: Confusion matrix details

S.No	Terminology	Description
1	**True Positives (TP)**	This means that both of the real class & predicted class of the data point is one.
2	**True Negatives (TN)**	This means that both of the real class & predicted class of the data point is Zero
3	**False Positives (FP)**	In this the real class of data point is zero & predicted class of data point is one.
4	**False Negatives (FN)**	In this the real class of data point is one & the predicted class of data point is zero.

Table-2: Confusion matrix terminology

S.No	Terminology	Description	Formula
1	**Classification Accuracy**	This is the most frequently used performance metric for algorithms classifications. This is defined as the total numbers of correct predictions created and divided by the total predictions and calculated at its percentage value	Accuracy = TP + TNTP + FP + FN + TN
2	**Classification Report**	This report is made to calculate the performance of the scores	
2.1	**Precision**	It is used in finding the correct results, this can be defined as the total number of correct results returned by the ML model.	Precision= TPTP + FP
2.2	**Recall**	Recall is termed as the total number of positives returned by the ML model.	Recall= TPTP + FN
2.3	**Specificity**	It is in contrast with the recall value recall, it can be defined by the number of negatives value returned in the ML model.	Specificity = TNTN + FP
2.4	**Support**	It is measured as the number of samples of the genuine response within each class	
2.5	**F1 Score**	F1 score give us the mean value.	$\boldsymbol{F1} = \mathbf{2} * (\boldsymbol{precision} * \boldsymbol{recall}) / (\boldsymbol{precision} + \boldsymbol{recall})$
		F1 score is having equal relative contribution of precision and recall.	

Workflow of the research Proposal

The Table 3 represent the thesis plan

Table-3: Thesis Plan

	Thesis Approach			
Step 1	**Step-2**	**Step-3**	**Step-4**	**Step-5**
Data Pre-processing	Feature Extraction	Missing value identification	Categorical Features	Visualization
Importing libraries and reading features list	Shape of data frame and getting data type of each feature	Finding missing values of all features.	Finding Categorical Features	Visualizing Categorical Features using bar graph

Step-6	**Step-7**	**Step-8**	**Step-9**	**Step-10**	**Step-11**
Feature Distribution	Data Correlation	Remove irrelevant features	Data Modelling	Various ML & DL Algorithms application	Analysis of result
Target the Feature Distribution based on the datasets	Find the highly correlated datasets by utilizing the heatmap analysis	Remove the Irrelevant Features from the dataset	splitting the dataset & model them	Apply various machine learning classification algorithms on the dataset	Analyse the training and testing accuracy of each model.

7. Requirements Resources

- Dataset
- Google Collab
- Laptop with minimum 16 GB Memory, 8 Core CPU & Inbuild GPU’s
- Jupyter Notebook

8. Research Plan

The Table 4 represents the proposed project plan

Table-4: Thesis Project Plan

CATEGORY	TASK	START	END
Pre-Implementation	Data Acquisition	5-1-22	5-15-22
	Prepare the problem	5-1-22	5-15-22
	Load libraries	5-1-22	5-15-22
	Load dataset	5-1-22	5-15-22
Summarize Data			
	Descriptive statistics	5-16-22	5-30-22
	Data visualizations	5-16-22	5-30-22
Prepare Data			
	Data Cleaning	5-31-22	6-16-22
	Feature Selection	5-31-22	6-16-22
	Feature Engineering	5-31-22	6-16-22
Evaluate Algorithms			
	Split-out validation dataset	6-17-22	7-16-22
	Test options and evaluation metric	6-17-22	7-16-22
	Compare Algorithms	6-17-22	7-16-22
Improve Accuracy			
	Algorithm Tuning	7-17-22	7-30-22
	Ensembles	7-17-22	7-30-22
Finalize Model			
	Predictions on validation dataset	8-1-22	8-30-22
	Create standalone model on entire training dataset	8-1-22	8-30-22
	Report Submission	8-1-22	8-30-22

1. References

10 Types of Cyber Attacks You Should Be Aware in [2021]. (n.d.). Retrieved May 3, 2022, from https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

Baldini, G., & Amerini, I. (2022). Online Distributed Denial of Service (DDoS) intrusion detection based on adaptive sliding window and morphological fractal dimension. *Computer Networks*, *210*, 108923. https://doi.org/https://doi.org/10.1016/j.comnet.2022.108923

Bangui, H., & Buhnova, B. (2022). Lightweight intrusion detection for edge computing networks using deep forest and bio-inspired algorithms. *Computers and Electrical Engineering*, *100*, 107901. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.107901

Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabé, J. B., Baldini, G., & Skarmeta, A. (2022). Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks*, *203*, 108661.

https://doi.org/https://doi.org/10.1016/j.comnet.2021.108661

Commonly Used Machine Learning Algorithms | Data Science. (n.d.). Retrieved May 3, 2022, from https://www.analyticsvidhya.com/blog/2017/09/common-machine-learning-algorithms/

Guarascio, M., Cassavia, N., Pisani, F. S., & Manco, G. (2022). Boosting Cyber-Threat Intelligence via Collaborative Intrusion Detection. *Future Generation Computer Systems*. https://doi.org/https://doi.org/10.1016/j.future.2022.04.028

Gupta, S. K., Tripathi, M., & Grover, J. (2022). Hybrid optimization and deep learning based intrusion detection system. *Computers and Electrical Engineering*, *100*, 107876. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.107876

Impact of cyber attack on your business | nibusinessinfo.co.uk. (n.d.). Retrieved May 3, 2022, from https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

Intrusion Detection System (IDS) - GeeksforGeeks. (n.d.). Retrieved May 3, 2022, from https://www.geeksforgeeks.org/intrusion-detection-system-ids/

Kilincer, I. F., Ertam, F., & Sengur, A. (2022). A comprehensive intrusion detection framework using boosting algorithms. *Computers and Electrical Engineering*, *100*, 107869. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.107869

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing*, *164*, 55–68. https://doi.org/https://doi.org/10.1016/j.jpdc.2022.01.030

M .P ., R., Reddy, P. V. B., Thirukrishna, J. T., & Vidyadhari, C. (2022). Intrusion detection in big data using hybrid feature fusion and optimization enabled deep learning based on spark architecture. *Computers & Security*, *116*, 102668. https://doi.org/https://doi.org/10.1016/j.cose.2022.102668

McAfee report says cybercrime to cost world economy over $1 trillion | Business Standard News. (n.d.). Retrieved May 3, 2022, from https://www.business-standard.com/article/technology/mcafee-report-says-cybercrime-to-cost-world-economy-over-1-trillion-120120700249_1.html

Samriya, J. K., Tiwari, R., Cheng, X., Singh, R. K., Shankar, A., & Kumar, M. (2022). NETWORK INTRUSION DETECTION USING ACO-DNN MODEL WITH DVFS BASED ENERGY OPTIMIZATION IN CLOUD FRAMEWORK. *Sustainable Computing: Informatics and Systems*, 100746. https://doi.org/https://doi.org/10.1016/j.suscom.2022.100746

Saveetha, D., & Maragatham, G. (2022). Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning. *Pattern Recognition Letters*, *153*, 24–28. https://doi.org/https://doi.org/10.1016/j.patrec.2021.11.023

Top 10 Deep Learning Algorithms You Should Know in 2022. (n.d.). Retrieved May 3, 2022, from https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm

Refer: Harvard Referencing Guide