Development of Threat Hunting Model Using Machine Learning Algorithms for Cyber Attacks Mitigation

*Akinsola, J. E. T.
Department of Computer Sciences
First Technical University
Ibadan, Nigeria
akinsola.jet@tech-u.edu.ng

Olajubu, E. A.
Department of Computer Science and Engineering,
Obafemi Awolowo University
Ile-Ife, Nigeria.
emmolajubu@oauife.edu.ng

Aderounmu, G. A.
Department of Computer Science and Engineering,
Obafemi Awolowo University
Ile-Ife, Nigeria.
gaderun@oauife.edu.ng

***Abstract*—Threat hunting has become very popular due to the present dynamic cyber security environment. As there remains increase in attacks' landscape, the traditional way of monitoring threats is not scalable anymore. Consequently, threat hunting modeling technique is implemented as an emergent activity using machine learning (ML) paradigms. ML predictive analytics was carried out on OSTO-CID dataset using four algorithms to develop the model. Cross validation ratio of 80:20 was used to train and test the model. Decision tree classifier (DTC) gives the best metrics results among the four ML algorithms with 99.30% accuracy. Therefore, DTC can be used for developing threat hunting model to mitigate cyber-attacks using data mining approach.**

Keywords: Cyber attack, Decision tree, Machine learning, OSTO-CID dataset, Threat hunting

I. INTRODUCTION

In the present dynamic environment of cyber security, with its attack scenery that is changing rapidly, industries or organizations are increasingly being informed of the importance of being ahead of new trends of cyber threats. Threat hunting has become very popular due to this reason. A new type of threats has exceptionally become proficiently successful, such as interruptions that are not detected, system vulnerabilities exploitation, network defenses breaching as well as gaining access to organization's data and systems [1]. As there is an increase in attack landscape, a lot of security teams have discovered that the traditional way of responding to and monitoring threats is not scalable anymore. However, a forward-thinking search for attackers as well as weaknesses is needed for attacks prevention from escalating beyond recovery. As there is continuation of battlefield which evolves into the modern terrain of cyber security; there is a need to strive so hard to prevent attacks and this method has also evolved with the present wave of cyber threat hunters. Organizations that is very conscious of security are aware that the strongest defenses cannot position themselves as purely reactive, they must seek out the unidentified as well recognizing the unexpected before there is an evolvement of attack that goes beyond their control. Therefore, it is necessary to move beyond the buzzwords and hype; instead set realistic expectations for what a threat hunters is and what they are capable of achieving [2]. To achieve this, application of machine learning for threat hunting is highly desirable.

Machine learning (ML) is an important technique in the usage of data as well as huge technology for data mining in various fields like science, business and finance, healthcare and involves forecasting, decision making and prediction. It is an aspect of artificial intelligence (AI) that focuses on permitting computers to gain knowledge from data and for desired task performance automatically [3]. ML algorithms such as Support Vector Machines, Decision Tree, Random Forest and so on are used for individual classifier's performance improvement and to present a better and effective path of threat hunting [4]. The aim of this study therefore, is to proffer solution to the problem of cyber attack and to reduce the rate by which cyber criminals gain access to organization's data or network by developing a threat hunting model using ML algorithms such as Decision Tree, Multilayer Perceptron, Support Vector Machines as well as Gradient Boosting. This will greatly prevent cyber criminals and ultimately mitigate cyber attacks in the organizations.

Section 1 is concerned with the introduction to cyber threat hunting. Section 2 discusses the literature review, the work that has been done by different authors in relation to threat hinting and machine learning; and the aim and objectives of this research. Section 3 discusses the method used in carrying out the research, the steps taking in carrying out threat hunting, the tools used and analysis done on the data collected. Section 4 discusses the result of the analysis carried out on the data using machine learning algorithms in order to build the model and section 5 deals with the conclusion of this research.

II. RELATED WORK

Threat hunting is explained as an emergent activity that consists of the iterative, proactive as well as human-centric recognition of Information Technology regarding internal cyber attacks that have eluded the current controls of security [5]. It can also be defined as the proactive hypothesis that is driven by discovery of activity, artifacts or methods of detection that is not accounted for monitoring capabilities that

979-8-3503-2028-2/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCI58124.2022.00242

is passive [2]. There will be improvements in organizations that operate capability of threat hunting in their security posture; hence there will be reduction in risk such that activity that is malicious can be recognized earlier concerning attacks [5]. Threat hunting that is effective depends on a methodical approach and a mindset that permits the security analyst to reason like threat actor and then use the knowledge to determine what may identify an underway of attack. While experiencing certain helps, the changing landscape of threat actors as well as their sophistication, requires that threat hunter takes a strict approach that structures a methodical-based hunt on top of threat actors [6].

A. *Threat Hunting Tactics, Techniques and Procedures (TTPs)*

The processes or steps required for an efficient design of a successful hunt are discussed thus and Fig. 1 shows the control flow diagram of threat hunting model.

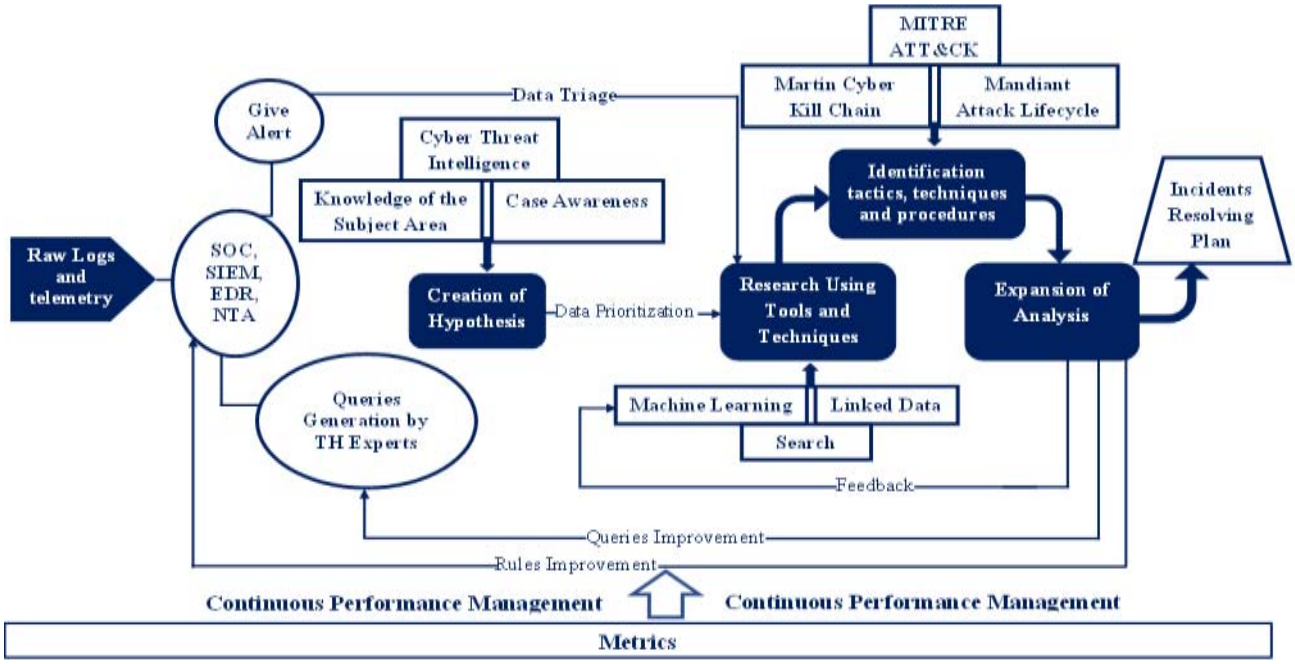

Fig. 1. Threat Hunting Model

1) Definition of Attack Scenario

In this phase the threat hunter should think through the whole TTPs that could be used, the targets within the network that could be attacked as well as several vulnerabilities that can be exploited by this type of attack.

2) Creation of Hypothesis: Hypothesis is the beginning of a threat hunts or a statement about the ideas of the hunter of what threat might be in the surrounding as well as how to go about identifying them. Hypothesis may consist of a suspected Threat Tactics, Techniques and Procedures of an attacker (TTPs). Threat hunters use their own threat intelligence, experience, environmental knowledge as well as their creativity to build a path of detection that is logical [7].

3) Investigating through Technique and Tools: After remarks have led to the generated hypothesis, then confirmation of remarks by means of all the suitable techniques as well as tools is required. Current tools obtained by organization for example Security Information and Event Management (SIEM) software or security analytic platform might not be adequate. Advance techniques of data science as well as visualizing data can be of help in detecting anomalies for threat hunters as well as identifying patterns [8].

4) *Uncover TTPs and New Patterns:* The output of investigating hypothesis is to proof if malicious activity is present or not. If not, it doesn't interpret that anomalous activities are not existing. Alternatively, the threat hunter may have not recognized any anomalies within the data that identifies the presence of activity that is malicious [5].

5) Inform and Enrich Analytics: Hunting process that is successful can be used for making effective decision for threat hunters to bring reduction in time of the threat hunting team as well as to reduce or prevent them from repetition of the similar process continuously. This could be carried out by scheduling a saved search, providing the supervised machine learning algorithms the necessary feedback or development of new analytic within present tools. The analytic platform for security should be allowed to repeat the successful hunting procedure from the precious operation of threat hunting. Also, it can be used for finding a new hypothesis by the threat hunter to expose the process of malicious act which is not detected before [8].

B. *Types of Threat Indicators*

The maturity model for detection of threat expresses that indicators of threat can be identified at different levels of semantic. High semantic indicators like goal and strategy or TTPs are more valuable to recognize than low semantic indicators for example, indicators and network artifacts like IP

addresses. SIEM tools provide only indicators at low levels of semantic relatively.

Threat indicators are of two types:

1) *Indicator of Comprise (IOC):* this indicator is an information on the signs of malicious activity, which is designed in a way that it can be fed into automated tools designed to look into the infrastructure for infectious signs [9]. IOC informs the threat hunters that an action has taken place and they are in reactive mode. All these unusual activities allow security administrators to identify malicious actors earlier in the process of cyber attack [10].

2) *Indicator of Concern*: data can be collected with the use of Open-Source Intelligence (OSINT) from available sources that are public to be used for detection of cyber attack and threat hunting [10].

C. Threat Hunting Methods

Methods or techniques used by threat hunters to identify threat or an attack in an organization is discussed below.

1) *Intelligence-Based Hunting* [11]**:** This is a reactive threat hunting technique designed to operate according to the source of input of intelligence. Intelligence like IP addresses, domain names, indicator of compromise as well as hash values. SIEM and threat intelligence tools can be integrated in this process to hunt for threats.

2) *Hypotheses Based Threat Hunting* [11]**:** Hypothesis threat hunting technique consists of testing three hypothesis types which are:

a) *Analytics-Driven:* this type of hypothesis makes use of user and entity behaviour analytics and machine learning for development of aggregated risk scores and hypothesis formulation.

b) *Intelligence-Driven:* this includes analysis of malware, scanning of vulnerability as well as intelligence feeds and reports.

c) *Situational-Awareness Driven:* this consist of analysis and risk assessments for identification of the digital assets that are essential to the company. The huge amount of data collected means that threat hunters need to play a big part in the process through the use of threat intelligence and machine learning.

3) *Investigation through Indicators of Attack (IoA***)** [11]**:** This is the most evident threat hunting technique that is proactive. Identification of Advanced Persistent Threat (APT) group is its first step of action as well as malware attacks through global detection by leveraging on playbooks. This method is mostly aligned with threat frameworks like MITRE ATTACK.

4) *Hybrid Hunting* [11]**:** All the three methodologies discussed above are combined together in this method to allow security analysts to customize the threat hunting. It incorporates industry-based hunting with awareness of the situation, combined with a particular hunting demand. For instance, the hunt can be customized using data about issues of geopolitics. Hypothesis can also be used as the trigger to leverage IoCs and IoAs.

D. Maturity Model of Threat Hunting

The maturity model of threat hunting was developed by David Bianco. There are five levels description of organizational hunting capability starting from Level 0 (the lowest capable level) to level 4 (the most capable level) [12] as shown in Fig. 2.

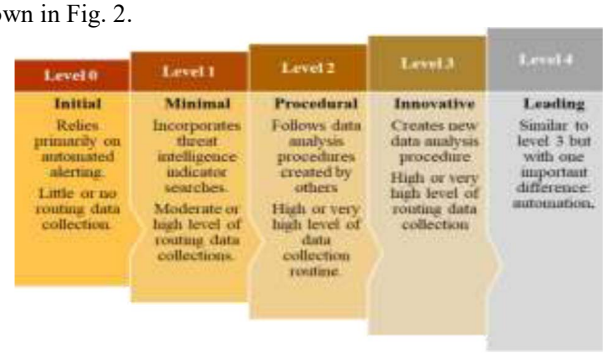

Fig. 2. Maturity Model of Threat Hunting

1) *Level 0 - Initial:* Organizations employ alerting solution that is automated in this level. For example, antivirus software, IDS or SIEM for malicious activities detection in the face of a corporate network [13].

2) Level 1 - Minimal: At this level, alerting guide that is automatic is being used frequently by organizations for their incident process response guidance. Though, the environment visibility gets much better, majorly thanks to large logs variety collections [14].

3) Level 2 - Procedural: Input data type that is expected is combined with a particular analysis method in this level for the discovery of malicious activity type; for example, malware detection through gathering of data that is related to which programs are automatically set to start hosting on [12].

4) Level 3 - Innovative: Organizations that have reached level 3 of maturity threat hunting model have the possibility of having good visibility into their network environment at the endpoint as well as network point. The organization that have reached this level can be put in place of Security Orchestration, Automation, and Response (SOAR); that is, an automation platform [15].

5) Level 4 - Leading: A company which has developed to level 4 of maturity threat hunting model is capable of maintaining ongoing operations of threat hunting [15].

E. Threat Hunting Metric

Dwell time is a powerful metric in the present cyber threat landscape for security teams to assess the whole process of operations of security program starting from architecture to engineering to operations as well as incident response. Dwell time can also be used as a transparent measure to assess how well the team, or the services of a service provider, detects, neutralizes and prevents threats. It is the time that exists between the first execution of malware within an organization and is identification [16]. Dwell time is described as the time from when an attack enters successfully to the environment of network to the time the attack is removed completely from the environment [17]. The author [18] used ransomware hunt that

unearthed a historic banking trojan as case study where a customer got in touch to inform that a vendor, they worked with had been affected by ransomware and they were worried if they are also being infected with the attack. The author [19] defined threat hunting as "know what to find" because threat hunting is an approach not a technology. The author analyzed two methods of threat hunting which are manual and automated methods and gives the steps needed in carrying out a successful threat hunting process.

The author [20] opined that a cyber threat hunting practical model explains threat hunting as analyst driven and practical procedure of searching for invader TTPs in an environment. Two SANS threat hunting reviews discovered that 60 percent of industries using tactics of threat hunting are identifying quantifiable advancement in cyber security functionality indicators. This author provides cyber threat hunting guide; that is, a proactive tactic to follow to protect network from cyber criminals.

F. Machine learning Algorithms Application in Threat Hunting

Machine learning (ML) is an important technology in the usage of data as well as huge data mining technology in various field like science, business and finance, healthcare and involve in forecasting, decision making and prediction. It is an aspect of artificial intelligence (AI) that focuses on permitting computer systems to gain knowledge from data as well as automatic performance of desired task [3]. ML is established to help computer understand the present, past, foretell or anticipate what will occur in the nearest future for unrecognized situations [21]. Machine learning for survival analysis is a study or research based on the notion that data analysis must be performed till an event of interest will occur [4]. ML algorithms such as Support Vector Machine, Decision Tree, Random Forest and so on are used for individual classifiers performance improvement and to present a better and effective path of threat hunting [4]. Machine learning is all about recognition of pattern. A cyber security artificial intelligence expert can identify inconsistences in conveyed data patterns. The AI may not identify the irregularity known as threat but the threat itself will trigger threat hunting. It can also bang the door on the data; that is, breaking pattern. However, the previous reinforcement will lead the AI to an excellent decision [22]. ML techniques is also used for extracting threat intelligence that is of high-level automatically from unlabeled sources [23].

III. MATERIALS AND METHODS

The material such as tools, dataset, ML algorithms and metrics used in this study and the methods of how they have been used are discussed in this section.

A. Dataset

The dataset known as ISOT Cloud Intrusion Dataset (ISOT-CID) was introduced publicly as the early solution towards addressing needs as well as creating way for communities of cloud security for more findings as well as research. The dataset contains over 2.5TB of dataset which include a wide range of attack vectors and normal activities. The ISOT-CID is a combination of several data collected from different cloud layers like hypervisors, guest hosts and networks. Also, it consist of data with several setups and from various sources of data which includes resource (for example, CPU), dumps of memory, utilization of logs, network traffic, system logs also from system call traces. It is huge and diverse enough for accommodating different data models of intrusion, feature sets as well as models of analyzation [24].

B. Tools

The tools such as packages and libraries used in carrying out analysis on the OSOT-CID dataset are Anaconda, Jupiter notebook and Scikit learn.

C. Machine Learning (ML) Algorithms

ML algorithms are models used by machine learning to carry out its operations on a given dataset. The algorithms used in this work are Decision Tree Classifier, Multilayer Perceptron, Support Vector Classifier as well as Gradient Boosting Classifier. The threat hunting architectural model developed for this study is shown on Fig. 1.

D. Performance Metrics

These are statistical measures for measuring the performance of a particular algorithms. The metrics used in this work are discussed below and as shown in equations (1) – (5).

1) Accuracy: This is the number of datasets that is predicted correctly out of all the datasets. It is described as the number of TN (true negatives) and TP (true positives) divided by the total number of TP, TN, FP (false positives) as well as FN (false negatives). A TP and TN is a dataset that is classified correctly by the ML algorithm as true or false while the FP and FN is a dataset that is not correctly classified by the algorithm [25]. Accuracy is one of important metrics required to get accurate performance evaluation analysis [26]. The formula in mathematical form is:

$$\text{Accuracy} = \frac{TN+TP}{TN+TP+FN+FP} \quad (1)$$

2) Kappa Statistics: This is how the data classified by the ML classifier are closely matched to the data labeled as ground truth is measured, whereby controlling the random classifier accuracy by the accuracy that is predicted [27].

$$\text{Kappa Statistics} = \frac{p_0-p_e}{1-p_e} \quad (2)$$

Where p_0 = observed accuracy and p_e = expected accuracy

3) Precision: This is also called positive predictive value [28]. This is the quality of the prediction that is positively made by the model [29]. It is the quantity of fault-prone classified dataset that are really fault-prone dataset [30]. The mathematical notation is:

$$\text{Precision} = \frac{TN}{TP+FP} \quad (3)$$

Where TN means True Negative, TP means True Positive and FP means False Positive.

4) Recall: The percentage of a certain correctly identified class from all the given examples of that class is known as recall. Recall is how complete are the search result [31]. It is calculated mathematically by TP divided by any class that should have been positively predicted that is TP and FN [32]. it is mathematically noted as:

$$\text{Recall} = \frac{TP}{TP+FN} \quad (4)$$

Where TP = True Positive and FN = False Negative.

5) F1 Score: It is the amount of how accurate an algorithm is on a dataset. It is used in the evaluation of binary classification systems which categorize example into negative or positive. It is a combination of recall and precision of the model. It is known as the harmonic mean of the recall and prediction value of a model [33].

$$\text{F1 Score} = 2 \times \frac{precision \times recall}{precision + recall} \quad (5)$$

TABLE 1. PERFORMANCE EVALUATION RESULTS USING CROSS VALIDATION RATIO OF 80:20

S/N	Machine Learning Algorithms	Accuracy (%)	Kappa statistics	Precision	Recall	F1 Score
1.	Decision Tree Classifier (DTC)	99.30	0.995	1.00	1.00	1.00
2.	Multilayer Perceptron (MLP)	51.20	0.053	0.55	0.51	0.51
3.	Support Vector Classifier (SVC)	69.00	0.355	0.69	0.69	0.69
4.	Gradient Boosting Classifier (GBC)	99.25	0.984	0.99	0.99	0.99

IV. RESULTS AND DISCUSSION

The machine learning metrics results were presented as shown in Table 1 using accuracy, kappa statistic, recall, precision, F1-score. Decision tree classifier gives accuracy of 99%, multilayer perceptron gives accuracy of 51%, support vector classifier gives accuracy of 69% and gradient boosting gives accuracy of 99%. Kappa statistic of decision tree classifier, multilayer perceptron, support vector classifier and gradient boosting classifier are 0.995, 0.53, 0.355 and 0.984 respectively.

Decision tree classifier gives 1.00 precision result, multilayer perceptron gives 0.51 precision result, support vector classifier of 0.69 precision result and 0.99 precision result by gradient boosting classifier. Recall result for the DTC, MLP, SVC also GBC are 1.00, 0.51, 0.69 and 0.99 respectively and F1 score result of 1.00 by decision tree classifier, 0.51 by multilayer perceptron, 0.69 by support vector classifier and 0.99 by gradient boosting classifier. Table1 shows the machine learning metrics result of the algorithms used in this research using 80:20 cross validation splitting ratio.

V. CONCLUSIONS

Threat hunting has become very popular due to the present dynamic environment of cyber security, with its attack scenery that is changing rapidly, industries or organizations are increasingly being aware of the importance of being ahead of new trends of cyber threat. Hence, to reduce the rate of cyber attacks in the organizations, machine learning analysis is carried out on OSTO-CID using four ML algorithms such as DTC, MLP, SVC as well as GBC using cross validation ratio of 80:20.

Comparative analysis was done on the result in order to determine the best algorithm for building a threat hunting model that can detect cyber attack effectively. From the metrics result produced by each algorithm; decision tree classifier gives the best result on all the machine learning metrics used in this research with 80:20 cross validation ratio. The results are: 99.30% accuracy, 0.995 kappa statistic, 1.00 for precision, recall and F1 score respectively. Therefore, the best machine learning algorithms to be used for developing threat hunting model using 80:20 cross validation ratio is Decision Tree Classifier.

Fig. 3, Fig. 4, Fig. 5, Fig. 6 and Fig. 7 shows the graphical representations of the results for each metric on 80:20 cross validation ratio.

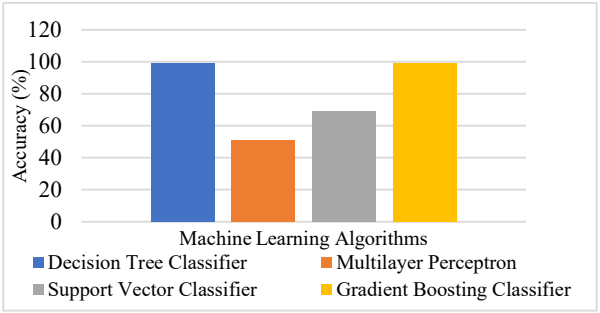

Fig. 3. Accuracy Result On 80:20 Splitting Ratio

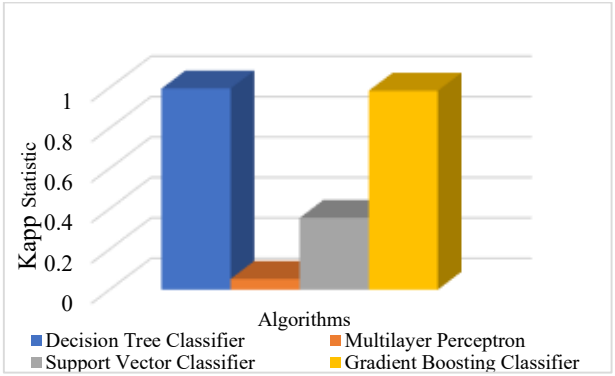

Fig. 4. Kappa Statistic Result on 80:20 Ratio

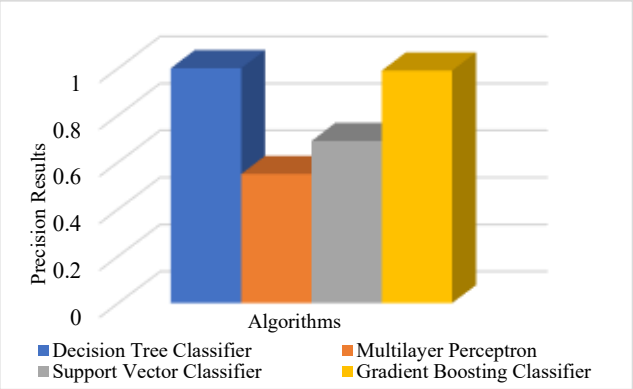

Fig. 5. Precision Result on 80:20 Ratio

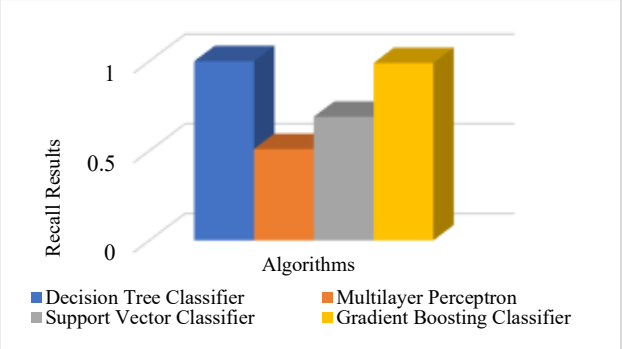

Fig. 6. Recall Result on 80:20 Ratio

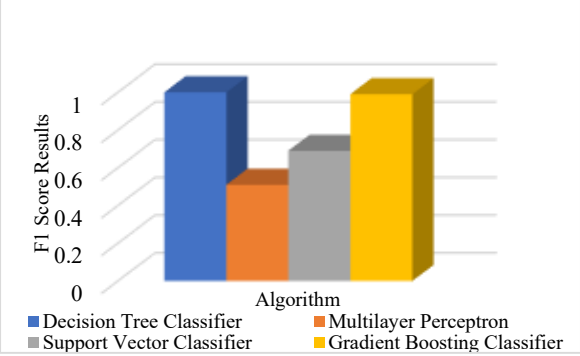

Fig. 7. F1 Score Result on 80:20 Ratio

REFERENCE

[1] A. Bhardwaj and S. Goundar, "A framework for effective threat hunting," *Netw. Secur.*, vol. 2019, no. 6, pp. 15–19, 2019, doi: 10.1016/S1353-4858(19)30074-1.

[2] Fidelis Cybersecurity, *THREAT HUNTING ESSENTIALS : Part 1 : Threat Hunting Defined*, vol. 6. 2020.

[3] J. E. T. Akinsola, O. Awodele, S. A. Idowu, and S. O. Kuyoro, "SQL Injection Attacks Predictive Analytics Using Supervised Machine Learning Techniques," *Int. J. Comput. Appl. Technol. Res.*, vol. 9, no. 4, pp. 139–149, 2020, doi: 10.7753/ijcatr0904.1004.

[4] Y. Shukla, "Threat Hunting Using a Machine Learning Approach Cyber Security," National College of Ireland, 2021.

[5] UK Government, "Detecting the Unknown: A Guide to Threat Hunting," *Hodigital*, vol. 2, no. 3, pp. 1–50, 2019.

[6] ChaosSearch, *The Threat Hunter ' s Handbook*. ChaosSearch, 2021.

[7] Trellix, "What Is Cyber Threat Hunting?," *Trellix*, 2022. .

[8] D. Oktavianto, "Cyber Threat Hunting Workshop," *ITU*, no. November, 2020.

[9] D. Makrushin, "Indicators of Compromise as an Instrument for Threat Intelligence," *Researchgate*, no. 08, pp. 1–9, 2021.

[10] Wikipedia, "Cyber threat hunting," *Wikipedia*, 2022. .

[11] O. Cassetto, "Threat hunting: Methodologies, Tools and Tips for Success," *Exabeam*, 2022. .

[12] Sqrrl Team, "The Threat Hunting Reference Model Part 1: Measuring Hunting Maturity," *Sqrrl*, pp. 1–3, 2015.

[13] F. Imam, "Threat hunting maturity model," *Infosec Resources*, 2018. .

[14] O. Rumiantseva, "Threat Hunting Maturity Model Explained With Examples," *SOC Prime*, 2022. .

[15] Blog, "Threat Hunting Maturity Model: A New Approach for Structured Hunting," *Cyborg Security*, 2021. .

[16] Infocyte, *Controlling dwell time*. Infocyte, 2016.

[17] ARMOR, *Dwell Time as a Critical Security Success Metric*, no. 04. ARMOR, 2020.

[18] Sophos, *Getting Started With Threat Hunting*, no. August. A Sophos Whitepaper, 2022.

[19] L. Pungur and G. H. Buck, *A pragmatic approach to curriculum*. rTHREAT, 2020.

[20] Tyler, *Guide To How To Take a Proactive Approach*. Tyler, 2018.

[21] J. E. T. Akinsola, M. A. Adeagbo, and A. A. Awoseyi, "Breast cancer predictive analytics using supervised machine learning techniques," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 6, pp. 3095–3104, 2019, doi: 10.30534/ijatcse/2019/70862019.

[22] U. Holmen, "AI and Machine Learning for Threat Detection," no. 823988. NTT, 2022.

[23] Y. Ghazi, Z. . supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources Anwar, R. Mumtaz, S. Saleem, and A. Tahir, "A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources," in *Proceedings - 2018 International Conference on Frontiers of Information Technology, FIT 2018*, 2019, no. 12, pp. 129–134, doi: 10.1109/FIT.2018.00030.

[24] A. Aldribi, I. Traore, P. G. Quinan, and O. Nwamuo, "Documentation for the ISOT Cloud Intrusion Detection Benchmark." University of Victoria, pp. 1–20, 2020.

[25] DeepAI, "Accuracy (error rate) Definition," *DeepAI*, 2020. .

[26] F. Y. Osisanwo, J. E. T. Akinsola, O. Awodele, J. O. Hinmikaiye, O. Olakanmi, and J. Akinjobi, "Supervised Machine Learning Algorithms : Classification and Comparison," vol. 48, no. 3, pp. 128–138, 2017.

[27] Stack Exchange, "classification - Cohen's kappa in plain English - Cross Validated," *Stack Exchange*, 2021. .

[28] Wikipedia, "Precision and recall," *Wikipedia*, 2022. .

[29] C3 AI, "Precision," *C3 AI*, 2022. .

[30] J. E. T. Akinsola, O. Awodele, S. O. Kuyoro, and F. A. Kasali, "Performance Evaluation of Supervised Machine Learning Algorithms Using Multi-Criteria Decision Making Techniques," in *International Conference on Information Technology in Education and Development (ITED)*, 2019, pp. 17–34, [Online]. Available: https://ir.tech-u.edu.ng/416/1/Performance Evaluation of Supervised Machine Learning Algorithms Using Multi-Criteria Decision Making %28MCDM%29 Techniques ITED.pdf.

[31] Stack Overflow, "statistics - What does recall mean in Machine Learning?," *Stack Overflow*, 2021. .

[32] A. Shafi, "What are the definitions of Precision and Recall?," *Towards Data Science*, 2022. .

[33] T. Wood, "F-Score Definition," *DeepAi.org*, 2019. .