NETWORK BASED ANOMALY DETECTION USING EFFICIENT MACHINE LEARNING ALGORITHM

V S Stency1 **and Dr. N Mohanasundaram** 2

1 Research Scholar, Depatment of CSE, Faculty of Engineering, Karpagam Academy of Higher Education, Coimbatore - 641021, Tamil Nadu, India.

2 Professor, Depatment of CSE, Faculty of Engineering, Karpagam Academy of Higher Education, Coimbatore- 641021, Tamil Nadu, India.

ABSTRACT

Network-based intrusion detection systems (NIDS) monitor and record information about incoming and outgoing internet traffic to identify potential security risks and compromises. The NIDS sensors in a network are purposefully spread throughout the network to maximize visibility. To obtain maximum visibility, sensors could be deployed on both the LAN and the DMZ. Network intrusion detection systems (NIDS) use a combination of signature- and anomaly-based detection methods to detect threats. Malware can be detected using the signature-based detection approach. This approach compares the properties of collected data packets to the characteristics of malicious signature files. Anomaly-based detection compares the behaviour of network events to a baseline of 'normal' network activity to identify patterns to find abnormalities. Using network intrusion detection systems (NIDS) technologies, which create alarms that can be used for further research, it is possible to spot malicious or aberrant network behaviour. There has been lot of research carried out to identify and prevent IDS by using machine learning algorithm. In this work we concentrate on the design and implementation of IDS by using efficient machine learning algorithm of SVM, NB, DT and logistic regression model. The performance has been analysed with the Accuracy, recall, f-measure and precision. Here the NSL-KDD cup data has been used for experimental work.

Keywords: KDD cup, SVM, NB, DT, logistic regression, machine learning, NIDS.

INTRODUCTION

Intelligent security technology on cloud infrastructure is needed to respond to recent network threats that are employing increasingly intelligent techniques. Since it is delivered ~~as~~ Security as a Service in a cloud setting, it helps small and medium businesses develop IT security solutions at a lower cost and with less effort. Recent cyber-attacks, such as DDoS, APT, and Ransomware, have infected the networks and resources of a number of small and medium-sized businesses (SMEs). These attacks either obliterate the infected systems and resources, or they obliterate the infected systems and in such cases, demand money in return for a decryption key. Ransomware is a form of ransomware that is used to extort money from. As a result, attackers can take advantage of the situation. The size of the damage caused by their attacks is

unimaginable, thanks to increasingly intelligent techniques. In today's world, there is an increasing demand for advanced security equipment and solutions that can identify and prevent threats. New security threats must be addressed. There is, however, a cap. to assisting small companies in making significant financial investments, Security specialists should be hired, and security technologies should be operated. As a result, Software Defined Security must be provided. Rather than using an existing hardware-based protection solution, (SDSec) services are used.

By receiving security services can increase security comparable to those of major corporations, but without the burden SecaaS is a forum for developing security solutions. It is important to build adaptive security service technologies in order to provide this personalised security service, a software-based security service that can dynamically reconfigure and analyse/respond intelligently. For this, we used cloud computing, which allows us to dynamically configure computing resources (network, server, storage, and so on) that a user needs. CIST stands for Cloud-based Intelligent Security Technology. Five components make up the personalised security service provisioning subsystems - (1) a dynamic reconfiguration control system (2) an analysis framework to detect and recognise the intelligent security threat, and (3) a complex compliance system a network virtualization and service chaining scheme, (4) a user experience management adapter, and (5) a bigdata adapter platform for gathering, processing, and storing security incidents a pile of logs

Intelligent threat detection is one of the services provided by intelligent protection. Analysis, malicious code detection, internal data leakage prevention, suspicious activity detection, and zero-day attack detection are only a few of the services available. Detection, for example, we put a lot of emphasis on this in this project. The identification and classification of network threats, which is a part of Intelligent threat analysis technology is a type of technology that analyses threats intelligently. We present a network threat detection and classification system based on the various machine learning algorithm, which is a component of intelligent threat analysis technology.

REVIEW OF THE LITERATURE

In 2020 the Huang, S., & Lei, Proposed a generative adversarial network towards intrusion detection systems in ad-hoc networks. The main contribution of the work concentrates on the class imbalance problem. In these 3 datasets of NSL-KDD, UNSW-NB15 and CICIDS2017 have experimented with FEED-forward network, the performance metrics of Accuracy, precision, recall, and f1-score have been evaluated with AUC curve. The results show that the proposed work outperforms the 15 other related work.

In 2020 the Punam BediNeha GuptaVinita Jindal. Deals with data imbalance problem for detecting intrusions. The main contribution of the work focuses on the data imbalance problem. a novel Imbalanced Siam-IDS neural network has been modeled with two data set of KDD and NSL-KDD. The proposed work concentrated the two different attack remote-to-local and user-to-root., the performance metrics of Accuracy, precision, the recall has been evaluated with two existing work of CNN and DNN. The results show that the proposed work of Siam-IDS efficiently carried out the data imbalance problem.

In 2014 the NedaAfzali SereshtRezaAzmi experimented with distributed IDS with the multi-agent-based Artificial immune system. The performance metrics of Accuracy, false alarm, and detection rate has been evaluated with the related work. The results show that the proposed work of the MAIS-IDS system performs efficiently.

In 2014 the J. Jabez B. Muthukumar experimented outlier-based detection method. The training model of the proposed work consists of big data set. The proposed work has also been evaluated with the KDD cup dataset. the performance metrics of CPU utilization, processing time detection time has been measured against the dataset. The result shows that the proposed work efficiently identifies the intrusions in the real-time environment.

In 2009 the Herrero, Á., Corchado, E., Pellicer, M. A., & Abraham, Deals with Mobile visualization induction taction system. The work deals with the multiagent based unsupervised IDS. The hybrid system work under many real-time situations on anomaly detection. The 3 datasets have been used for experimental purpose (PCA, MLHL, and CMLHL). The results show that the proposed work of MOVIES-IDS is efficiently carried out to detect the traffic on the IDS scenario.

In 2005 the OzgurDeprenMuratTopallarEminAnarimM. KemalCiliz experimented with hybrid IDS of the anomaly and misuse detection. The proposed work format both an anomaly and misuse detection with the decision support model. The work using many techniques to develop an efficient IDs system. the work using SOM, a Rule-based decision support system, and a j48 decision tree. The work experimented with the KDD cup dataset. The performance has been measured with detection rate, misuse classification, and misclassification with false-positive rate and compared with related work.

ARCHITECTURE OF THE PROPOSED WORK

Pre-processing

Imbalanced order includes creating prescient models on characterization datasets that have a serious class imbalance. The challenge of working with imbalanced datasets is that most AI methods will disregard, and thusly have horrible showing on, the minority class, albeit regularly it is execution on the minority class that is most important. One way to deal with

tending to imbalanced datasets is to oversample the minority class. The least difficult methodology includes copying models in the minority class, although these models don't add any new data to the model. All things considered; new models can be orchestrated from the current models. This is a kind of information growth for the minority class and is alluded to as the Synthetic Minority Oversampling Technique or SMOTE for short. SMOTE works by choosing models that are close in the component space, attracting a line between the models the element space and drawing another example at a point along that line.

Feature selection

The feature score provides a way to rank drivers based on the features that a driver supports. For example, feature scores might be defined for a device setup class that distinguishes between drivers based on class-specific criteria. The feature score supplements the identifier score, making it possible for driver writers to more easily and precisely distinguish between different drivers for a device that is based on well-defined criteria.

And even when you do have the incentive to hand-roll and -curate your features, automated feature selection provides some useful early directions for exploration during the exploratory process. The f-feature score-based feature selection is that allows to select features from a dataset using a scoring function. It supports selecting columns in one of a few different configurations: k for when you want a specific number of columns, percentile for when you want to a percentage of the total number of columns, and so on.

Feature selection methods are used to select the suitable feature subset from the overall dataset [16]. The main motive of this process is to select the relevant information and eliminate the irrelevant information from the dataset. The feature extraction provides better understanding for improving knowledge about the dataset. The overall computation cost has been reduced and the training process has also been reduced.

Classification

NAÏVE BAYES

The calculation for applying Bayes Theorem to a conditional probability classification model must be simplified. In the Bayes Theorem, each input variable is meant to be dependent on all other variables. This adds to the calculation's difficulty. Remove this assumption and treat each input variable separately from the others [15].

This transforms the model from a dependent to an independent conditional probability model, greatly simplifying the calculation. First, the denominator of the P (x1, x2,..., xn) equation is removed because it is a constant that is used to normalise the result and to quantify the conditional probability of each class for a specific instance.

The conditional probabilities of all variables with the same class label are then divided into conditional probabilities for each variable value with the same class label. The conditional variables that are independent are then multiplied. Consider the following scenario:

The calculation can be done for each of the class labels, with the highest probability label being chosen as the classification for the specific case. The maximum a posteriori, or MAP, decision rule [16] is the name given to this decision rule.

The Bayes Theorem is commonly used for classification and predictive modelling problems. Naive Bayes is a simplified version of the Bayes Theorem.

SUPPORT VECTOR MACHINE

Support Vector Machines (SVMs) are a broadly used approach in supervised studying of category and regression problems. However, it's miles generally utilized in gadget studying for category problems. The reason of the SVM set of rules is to discover the excellent line or selection boundary for destiny category of n-dimensional area into companies in order that new records factors may be effortlessly assigned to the appropriate group. The hyperplane [18] is the excellent assessment limit. The SVM is used to pick extrema / vectors that make contributions to the formation of the hyperplane.

Support vector machines are the call of the set of rules, and assist vectors are an excessive case. The reason of the guide vector gadget technique is to discover hyperplanes that separate records factors in N-dimensional area and distinguish their attributes) [19].

Subdivide kinds of records factors the use of extraordinary hyperplanes. Our purpose is to discover the extent with the biggest distinction or variety among the records factors in each category. Increasing the margin hole makes it less complicated to discover capability

The Logistic Regression Model

After the use of a metamorphosis characteristic, linear regression predictions are non-stop values (for example, rainfall in centimetres), however logistic regression predictions are discrete values (for example, whether a pupil exceeded or failed).

Logistic regression is high-quality acceptable for binary classification: records units wherein y = zero or 1, with 1 being the default magnificence, are the maximum common. As an example, while forecasting whether or not an occasion will take area or now no longer, there are simplest possibilities: that it takes area (which we denote as 1) or that it does now no longer take area (which we denote as 2). (zero). We could perceive ill sufferers the use of the fee 1 in our records set so that it will make a prediction approximately whether or not or now no longer a affected.

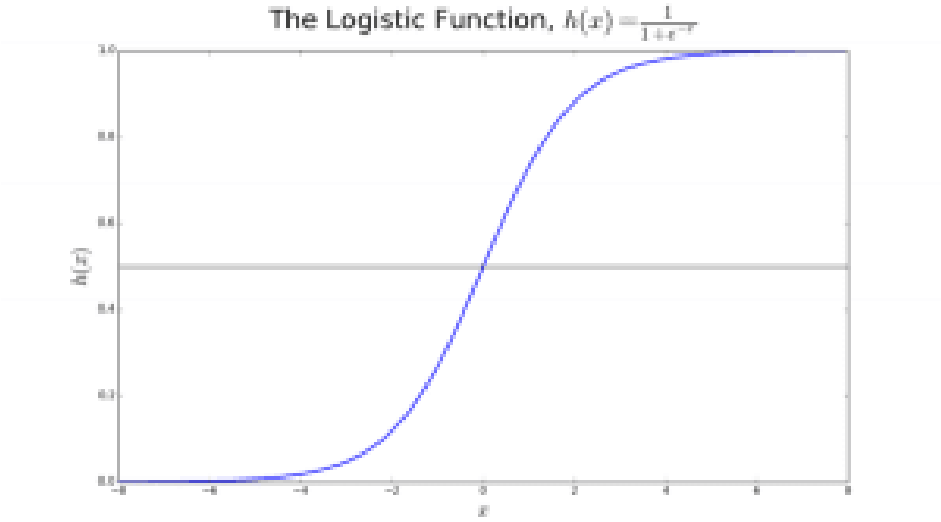

Figure 2 Logistic Regression

The logistic characteristic h(x)=1/ (1 + ex) is the transformation characteristic this is utilized in logistic regression, and it is called after that transformation characteristic. As a result, an S-formed curve is formed. If you run a logistic regression, the output is supplied as chances for the default magnificence of the model (in contrast to linear regression, in which the output is immediately produced). Due to the truth that it's far a possibility, the output will fall among zero and 1. If we`re looking to forecast whether or not sufferers are ill, for example, we already realize that ill sufferers are denoted through the quantity 1, consequently if our set of rules assigns a affected person the rating of zero.98, it believes that affected person could be very probable to be ill.

It is viable to attain this output (y-fee) through log-reworking the x-fee the use of the logistic characteristic h(x)=1/ (1 + e-x) and using the logistic characteristic h(x). After that, a threshold is used so that it will pressure this possibility right into a binary categorization system.

DECISION TREE

As opposed to unsupervised machine learning, Decision Trees are a type of Supervised Machine Learning (in which you explain what the input data is and what the related output data is in the training data) in which the data is continually segregated according to a specific parameter. The structure of the tree can be explained using two entities: decision nodes and leaves.

The leaves reflect the decisions or final outcomes. The decision nodes, on the other hand, are the sites where the data is divided. It's a versatile tool with several applications in a variety of industries. Classification and regression problems can both be solved with decision trees. In fact, the word implies that it uses a flowchart structure to illustrate the predictions that arise from a series of feature-based splits, similar to a tree structure. It starts with a root node and ends with the tree's leaves making a decision.

Algorithm For Decision Tree

- ✔ By clicking on it, you can make the tree's root node.
- ✔ The leaf node 'positive' is returned if all of the examples are positive.
- ✔ Otherwise, the leaf node 'negative' is returned if all of the cases are negative.
- ✔ Make a calculation of the current state's entropy H. (S)
- ✔ Make a note of the entropy of each attribute in relation to the attribute 'x' designated by H for each attribute (S, x)
- ✔ Choose the attribute with the greatest possible IG value (S, x)
- ✔ Subtract the attribute with the highest IG from the total number of attributes.
- ✔ Continue until the decision tree reaches its maximum number of leaf nodes, or we've exhausted all available attributes.

IMPLEMENTATION RESULTS AND ANALYSIS

This phase gives the experimental outcomes of our 4 gadget mastering strategies with 5 magnificence category methodologies the usage of NSL-KDD Cup intrusion detection datasets to hit upon community intrusions. Then a contrast with the present tactics is made to assess the efficacy of our intrusion detection model

Table 1 Performance Comparison

Method	Accuracy	Precision	Recall	F1 Score
Naive Bayes (NB)	87.7	87.3	84.3	86.7
Support Vector Machine (SVM)	88.7	90.4	87.9	89.1
Logistic regression	89.2	90.4	94.8	93.1
Decision Tree (DT)	93.3	92.3	93.4	94.3

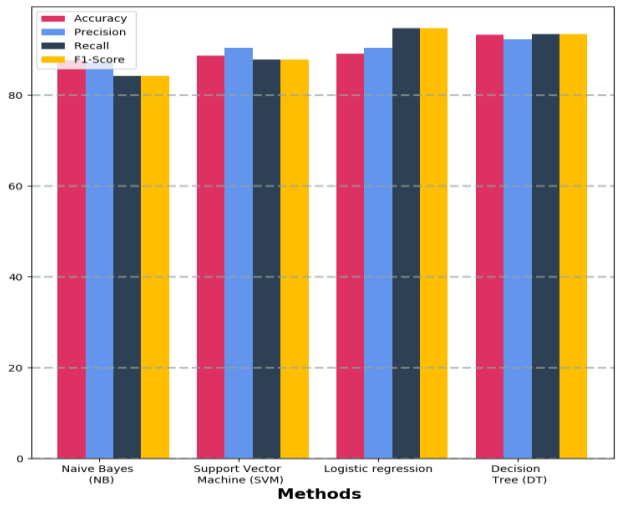

Figure 2 Performance Analysis

The overall performance has been analysed in table 2 figure 2. The table 3 describes the accuracy It is most common performance metric for classification algorithms. It may be defined as the number of correct predictions made as a ratio of all predictions made.figure 3 depicts parameter explanation of anticipated model

Table 3 Performance comparison of accuracy

Method	Accuracy
Naive Bayes (NB)	87.7
Support Vector Machine (SVM)	88.7
Logistic regression	89.2
Decision Tree (DT)	93.3

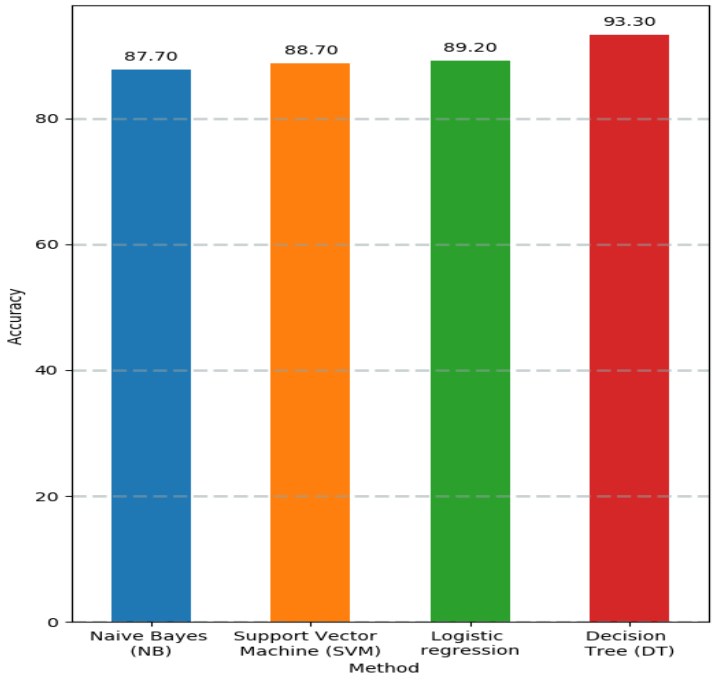

Figure 3 Performance Analysis Accuracy

The next performance has been describing precision, recall and f-measureThis score shows a harmonious average of accuracy and recognition. Mathematically, the F1 score is a weighted average of accuracy and memory. F1 scores make the same relative contribution to accuracy and memory. Once your model (classification model) is ready, you may want to find a work point.

Table 4 Performance Comparison Of Precision

Method	Precision
Naive Bayes (NB)	87.3

Support Vector Machine (SVM)	90.4
Logistic regression	90.4
Decision Tree (DT)	92.3

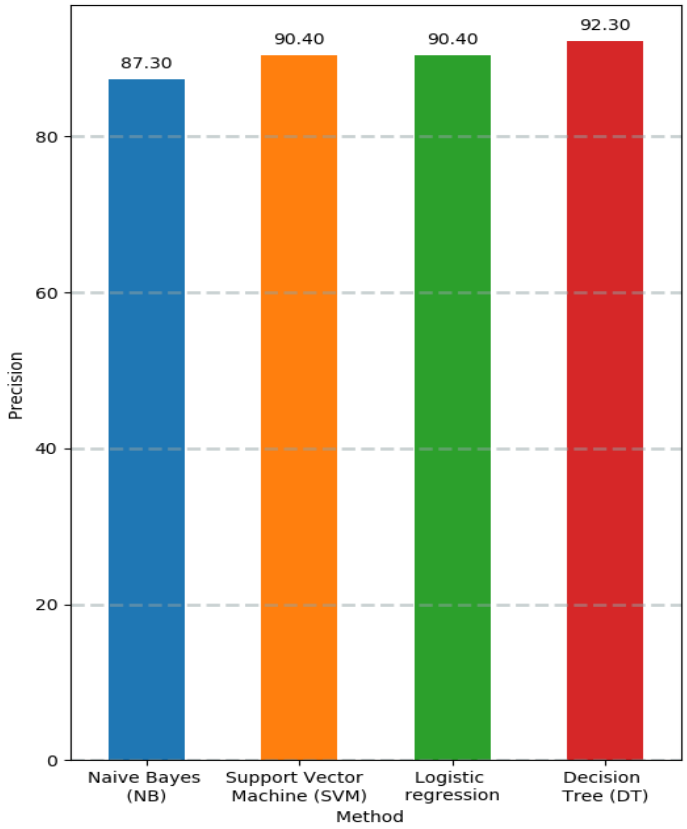

Figure 4 Performance Analysis Precision

. The table 4 describes the precision with the analysis model described in the figure 3 This is a trade-off between accuracy (higher thresholds are higher) and memory (higher thresholds are lower).the table 4 describes the recall and 6 describes the f-score .

Table 5 Performance Comparison Of Recall

Method	Recall
Naive Bayes (NB)	84.3
Support Vector Machine (SVM)	87.9
Logistic regression	94.8
Decision Tree (DT)	93.4

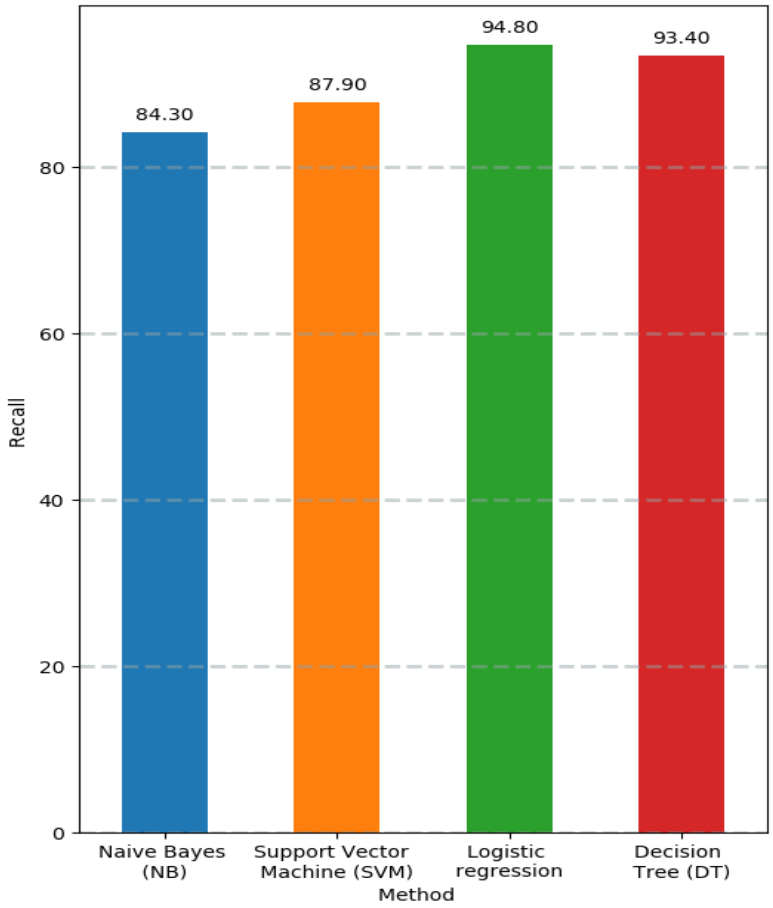

Figure 5 Performance Analysis Recall

Table 6 Performance Comparison Of F1 -Score

Method	F1 Score
Naive Bayes (NB)	86.7
Support Vector Machine (SVM)	89.1
Logistic regression	93.1
Decision Tree (DT)	94.3

The outcomes are appropriate for the feature types. Precision, accuracy, and recall value are evaluated and compared with each.

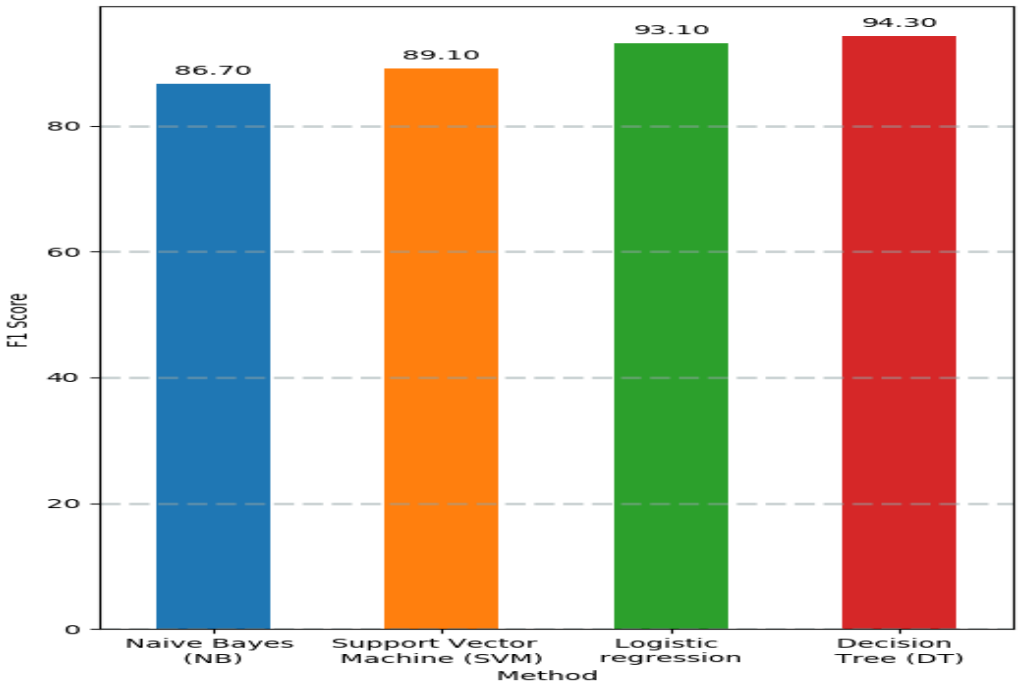

Figure 6 Performance Analysis F1-Score

Conclusion

Security in network is more important and a key factor for establishing the degree of trust. Network community needs to guarantee the security of data stored and performance through Quality of service. An enormous amount of models has been investigated to assure security. Identification and prediction of threats that influence the network communication have to be tackled effectively. This work mainly concentrates on network threat detection and classification using the various machine learning algorithm. To enhance the performance by identifying the legitimate users (legitimate, non-legitimate and partially legitimate) and detecting the threat, this works cast-off various machine learning algorithms such as Efficient Naive Bayes classifier, Improved Support vector machine, DT Logistic Regression. Initially, to monitor the incoming data, an effectual feature selection method has to be identified. After recognizing the sensitive data (i.e. threat awareness, sensitive information), classification is performed. By doing this, the degree of trust level has been increased amongst the cloud user community. The work's future development will focus on all the communication layers. Intrusion detection is primarily focused on the Application layer in this method, as the Application layer lacks any intrinsic intrusion detection capabilities.

References

[1]. Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E. and Song, Z. 2010. "Authentication in the Clouds: A Framework and its Application to Mobile Users", ACM CCSW'10, October 8, 2010, Chicago, Illinois, USA. pp. 1-6.

[2]. Chraibi, M., Harroud, H., and Maach, A. 2013. "Classification of Security Issues and Solutions in Cloud Environments", ACM iiWAS2013, 2-4 December, 2013, Vienna, Austria.

[3]. Houmansadr, Amir, Saman Zonouz, and Robin Berthier. "A cloud based intrusion detection and response system for mobile phones." In Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on, pp. 31-32. IEEE, 2011.

[4]. Ibrahim, Laheeb Mohammad. "Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN)." Journal of Engineering Science and Technology 5, no. 4 (2010): 457-471.

[5]. Emeakaroha, V.C., Netto, M.A.S., Calheiros, R.N., Brandic, I., Buyya, R. and Rose, C.A.F. 2012. "Towards autonomic detection of SLA violations in Cloud infrastructures", Future Generation Computer Systems (28), pp. 1017–1029.

[6]. Garcia-Morchon, O., Kuptsov, D., Gurtov, A. and Wehrle, K. 2013. "Cooperative security in distributed networks", Computer Communications (36), pp. 1284–1297

[7]. Hashemi, S.M. and Ardakani, M.R.M., 2012. "Taxonomy of the Security Aspects of Cloud Computing Systems – A Survey", International Journal of Applied Information Systems, (4:1), pp. 21-28.

[8]. Ali, M., Khan, S.U. and Vasilakos, A.V., 2015. Security in cloud computing: Opportunities and challenges. Information Sciences, 305, pp.357-383.

[9]. R. Bace, P. Mell, "Intrusion Detection Systems", National Institute of Standards and Technology (NIST), Technical Report,(2001), pp. 800 -31.

[10]. Roschke, S., Cheng, F. and Meinel, C., 2009, August. An extensible and virtualization-compatible IDS management architecture. In Information Assurance and Security, 2009. IAS'09. Fifth International Conference on (Vol. 2, pp. 130-134). IEEE.

[11]. Yang, Changsong, Xiaoling Tao, Feng Zhao, and Yong Wang. "Secure data transfer and deletion from counting bloom filter in cloud computing." *Chinese Journal of Electronics* 29, no. 2 (2020): 273-280.

[12]. Liu, Yudong, Shuai Xiao, Han Wang, and Xu An Wang. "New provable data transfer from provable data possession and deletion for secure cloud storage." *International Journal of Distributed Sensor Networks* 15, no. 4 (2019): 1550147719842493.

[13]. Yang, Changsong, Xiaoling Tao, and Feng Zhao. "Publicly verifiable data transfer and deletion scheme for cloud storage." *International Journal of Distributed Sensor Networks* 15, no. 10 (2019): 1550147719878999.

[14]. Wang, Yong, Xiaoling Tao, Jianbing Ni, and Yong Yu. "Data integrity checking with reliable data transfer for secure cloud storage." *International Journal of Web and Grid Services* 14, no. 1 (2018): 106-121.

[15]. Moloja, Dina, and Noluntu Mpekoa. "Towards a cloud intrusion detection and prevention system for m-voting in South Africa." In *2017 International Conference on Information Society (i-Society)*, pp. 34-39. IEEE, 2017.

[16]. Jelidi, Mohamed, Abdallah Ghourabi, and Karim Gasmi. "A hybrid intrusion detection system for cloud computing environments." In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pp. 1-6. IEEE, 2019.

[17]. Sakr, Mahmoud M., Medhat A. Tawfeeq, and Ashraf B. El-Sisi. "Network intrusion detection system based PSO-SVM for cloud computing." *International Journal of Computer Network and Information Security* 10, no. 3 (2019): 22.

[18]. Visniakou, U. A., Hani HJ Al-Musawi, ZR AL-ATTAR ABDULRAOUF, and RKH KHUDIER. "Analysis and applications of information security incorporate information system, cloud computing and blockchain." *ББК 32.811. 4 К57* (2020): 15.

[19]. Aljamal, Ibraheem, Ali Tekeoğlu, Korkut Bekiroglu, and Saumendra Sengupta. "Hybrid intrusion detection system using machine learning techniques in cloud computing environments." In *2019 IEEE 17th international conference on software engineering research, management and applications (SERA)*, pp. 84-89. IEEE, 2019.

[20]. Kale, Devendra P., and V. M. Thakare. "A Novel Approach to Design the Intelligent Technique for Intrusion Detection In Cloud."

[21]. Kanimozhi, V., and T. Prem Jacob. "Artificial intelligence-based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing." In *2019 international conference on communication and signal processing (ICCSP)*, pp. 0033-0036. IEEE, 2019.

[22]. Idhammad, Mohamed, Karim Afdel, and Mustapha Belouch. "Distributed intrusion detection system for cloud environments based on data mining techniques." *Procedia Computer Science* 127 (2018): 35-41.

[23]. Mohammadpour, Leila, Teck Chaw Ling, Chee Sun Liew, and Chun Yong Chong. "A convolutional neural network for network intrusion detection system." *Proceedings of the Asia-Pacific Advanced Network* 46, no. 0 (2018): 50-55.

[24]. Almiani, Muder, Alia AbuGhazleh, Amer Al-Rahayfeh, Saleh Atiewi, and Abdul Razaque. "Deep recurrent neural network for IoT intrusion detection system." *Simulation Modelling Practice and Theory* 101 (2020): 102031.

[25]. Yang, X.,(2009), 'Firefly Algorithm for Multimodal Optimization, SAGA 2009, LNCS 5792,pp.169-178,2009

[26]. Zang et al.,(2010), "A Review of Nature Inspired Algorithm" Journal of Bionic Engineering 7 Suppl. (2010)

[27]. Bilge, Leyla, and Tudor Dumitraş. "Before we knew it: an empirical study of zero-day attacks in the real world." In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 833-844. 2012.

[28]. Holm, Hannes. "Signature based intrusion detection for zero-day attacks:(not) a closed chapter?." In 2014 47th Hawaii international conference on system sciences, pp. 4895-4904. IEEE, 2014.

[29]. Lamba, Anil, Satinderjeet Singh, and Singh Balvinder. "Mitigating zero-day attacks in IoT using a strategic framework." International Journal for Technological Research in Engineering 4, no. 1 (2016).

[30]. Zhang, Mengyuan, Lingyu Wang, Sushil Jajodia, Anoop Singhal, and Massimiliano Albanese. "Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks." IEEE Transactions on Information Forensics and Security 11, no. 5 (2016): 1071-1086.

[31]. Portokalidis, Georgios, Asia Slowinska, and Herbert Bos. "Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation." ACM SIGOPS Operating Systems Review 40, no. 4 (2006): 15-27.

[32]. Boetto, Erik, Maria Pia Fantini, Aldo Gangemi, Davide Golinelli, Manfredi Greco, Andrea Giovanni Nuzzolese, Valentina Presutti, and Flavia Rallo. "Using altmetrics for detecting impactful research in quasi-zero-day time-windows: the case of COVID-19." Scientometrics (2021): 1-27.

[33]. Sohi, Soroush M., Jean-Pierre Seifert, and Fatemeh Ganji. "RNNIDS: Enhancing network intrusion detection systems through deep learning." Computers & Security 102 (2021): 102151.

[34]. Kamati, Toivo Herman, Dharm Singh Jat, and Saurabh Chamotra. "Design and Development of System for Post-infection Attack Behavioral Analysis." In Proceedings of Fifth International Congress on Information and Communication Technology, pp. 554-565. Springer, Singapore, 2021.

[35]. Garcia, Norberto, Tomas Alcaniz, Aurora González-Vidal, Jorge Bernal Bernabe, Diego Rivera, and Antonio Skarmeta. "Distributed real-time slowdos attacks detection over encrypted traffic using artificial intelligence." Journal of Network and Computer Applications 173 (2021): 102871.

[36]. Bokka, Raveendranadh, and Tamilselvan Sadasivam. "Deep Learning Model for Detection of Attacks in the Internet of Things Based Smart Home Environment." In Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, pp. 725-735. Springer, Singapore, 2021.

[37]. Singh, Geeta, and Neelu Khare. "A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques." International Journal of Computers and Applications (2021): 1-11.

[38]. Aksoy, Muhammet, Orhan Ozdemir, Guney Guner, Baris Baspinar, and Emre Koyuncu. "Flight Trajectory Pattern Generalization and Abnormal Flight Detection with Generative Adversarial Network." In AIAA Scitech 2021 Forum, p. 0775. 2021.

[39]. Adtiya Nur Cahyo ,Risanuri Hidayat, and Dani Adhipta, “Performance Comparison of Intrusion Detection System based Anomaly Detection using Artificial Neural Network and Support vector Machine ”, Advances of science and technology for society,978-0-7354-1413-6,doi-10.10631/1.4958506,2016.

[40]. Salima Omar, Asri Ngadi, and Hamid H. Jebur , “Machine Learning Techniques for Anomaly detection: An Overview”, Internation Journal of Computer Application,ISSN: 0975-8887, Volume 79-No.2 October, 2013.

[41]. Sergay Andropov, Alexei Guirik, Mikhail Budko and Marina Budko, “Network Anomaly Detection using Artificial Neural Network ”,Open Innovation Association(FRUCT) 20th Conference,2017,ISSN NO:2305-7254,IEEE 2017.

[42]. Mrutyunjaya Panda and Manas Ranjan Patra, “Network Intrusion Detection Using Naïve Bayes ”, International Journal of Computer science and Network Security, Vol. 7, No. 12, December 2007.

[43]. Manjiri V. Kotpalliwar and Rakhi Wajgi, “Classification of Attacks Using Support Vector Machine (SVM) on KDDCUP'99 IDS Database”, Fifth International Conference on Communication Systems and Network Technologies, 978-1-4799-1797-6, pp: 987-990, April