Impact and Feasibility of harnessing AI and ML in the realm of Cybersecurity to detect Network Intrusions: A Review

Swathi Dayanand, Chaitra Nagaraj

Abstract**:** ***Remarkable advances in cyberspace, have amassed a magnanimous set of Internet users worldwide. While people engage in various activities and use the web for various needs, the prospective fear of cyber attacks, crime and threats is indubitable. Though a plethora of preventive measures are in use, it is impossible to circumvent cyber threats completely. Cybersecurity is a domain that deals with prevention of cyber attacks by use of effective precautionary and remedial measures. With the advent of Artificial Intelligence (AI) and Machine Learning (ML) and its profound scope in contemporary technical innovations, it is a critical necessity to inculcate its techniques in enhancement of existing cybersecurity techniques. This paper offers a detailed review of the concepts of cybersecurity, commonly encountered cyber attacks, the relevance of AI and ML in cybersecurity along with a comparative performance analysis of distinct ML algorithms to combat network anomaly detection and network intrusion detection.***

Keywords: Cyber Security, Machine Learning, Network Anomaly Detection, Network Intrusion Detection

I. INTRODUCTION

Recently, cybersecurity has become a common term that has gained much attention and significance in the field of Information Technology(IT). However, the term cybersecurity has many subjective definitions which indicates that its relevance is multidimensional. In general sense, cybersecurity is concerned with protecting and safeguarding data, information and assets to prevent theft, loss or hampering. In other words, it also refers to techniques adopted to secure cyberspace and cyberspace-enabled devices from any kind of harmful actions intended to cause a breach of security or unauthorised access to confidential resources. Sometimes, cybersecurity is also articulated as a domain of knowledge dedicated to the study and practice of principles concerned with protection of digital assets.[1] (Craigen et al., 2014) As more business activities drift towards aspects of automation and computers have become indispensable, the need for cybersecurity has accentuated by leaps and bounds. Apparently, as more devices are being connected and accessed over the Internet, the task of safe-keeping critical data owned by governments, business organizations, and millions of daily users is of paramount importance. A computer network under the tutelage of aforesaid entities is vulnerable to attacks and threats which can be thwarted by adopting suitable measures of cybersecurity. Over the years, the evolution of a network towards a pervasive computational infrastructure has been undeniable. As networks today are becoming larger, complex and dynamic, cybersecurity has gained a cardinal status even accounting for national security measures.[2] (R. A. Kemmerer, 2003)

II. THREATS TO CYBERSECURITY

The exponential growth of the Internet and rising cyberspace usage has attributed to a considerable rise in cyber attack eventualities with a calamitous and grave aftermath. Cyber attacks are often deciphered by the nature and impact of its occurrence and classified on the basis of its origin in a computer network or Internet.[3] (Jang-Jaccard et al., 2014) The Symantec Security Summary 2020 has stated that amongst the 750 IT and cybersecurity professionals who were surveyed, 78% of them relied on 50 or more discrete solutions and techniques to deal with security issues while nearly 37% of them are dependent on over 100 tools for security. [4] The Cyber Security Report 2020 remarks that the biggest takeaway from the year 2019 is that every organization albeit it's employee strength is not completely immune to cyber threats and attacks. Cyber exploits have become more advanced, lethal, deceptive than ever before. An approximate value of US $ 1.5 trillion generated from cyber crimes in the year 2018, hints that the cyber landscape today is vulnerable to attacks and requires state of the art cyber security solutions. [5]

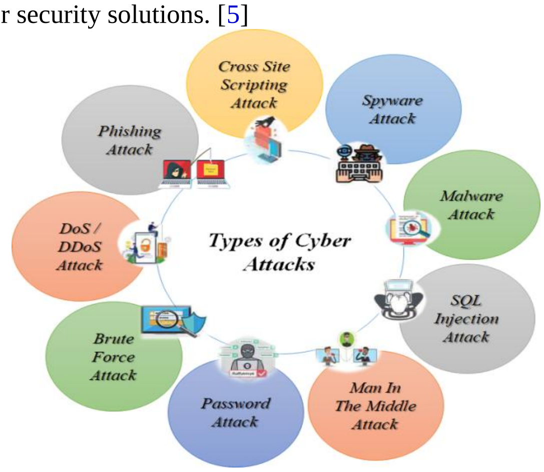

Fig. 1 The most common types of cyber attacks

Manuscript received on 26 June 2022 | Revised Manuscript received on 01 July 2022 | Manuscript Accepted on 15 July 2022 | Manuscript published on 30 July 2022.

* Correspondence Author

Swathi Dayanand*, Security Network Consulting Engineer, Aryaka Networks, Bengaluru (Karnataka), India.

Dr. Chaitra N, Associate Professor, Department of Electronics and Communication Engineering, BNM Institute of Technology, Bengaluru (Karnataka), India.

Retrieval Number: 100.1/ijrte.B71500711222
DOI: 10.35940/ijrte.B7150.0711222
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The most common types of cyber attacks are, [6] (Bendovschi et al., 2015), [7] (Biju et al., 2019, [8] (Fischer et al., 2014), [9] (Hussain et al., 2020), [10] (Pogrebna et al., 2019).

1. Man in the middle Attack : It is a common term used to describe an attack where a message exchange between two users or between a user and a network is intercepted by a perpetrator unknown to them. The aim of the offender is to eavesdrop on the information exchange or masquerade as a user, giving the false impression that there is no lapse of secrecy.

2. Cross Site Scripting Attack [XSS Attack] : It is a type of security infringement encountered in web applications which allows an attacker to inject malicious scripts into trustworthy and ethical web pages. This attack is manifested through the exchange of harmful code by an attacker in the form of a browser side script to a different end user using a web application.

3. Spyware Attack: Spyware is vaguely defined as a malicious software intended to enter a user system to collect personal data and expose it to third parties without the consent of the user. Spyware attack is a consequence of loss or misuse or illicit forwarding of user data by the spyware.

4. Malware Attack: It is a common cyberattack where a malware infiltrates a user system and leads to execution of unauthorised actions. It usually exploits or captures data from a device or a network to be leveraged for a profit.

5. SQL Injection Attack: It is a common loophole of web security that enables an attacker to intervene with the queries made by an application to its database. It permits the attacker to view non-retrievable data. Yet, there is a probability that the data in the SQL database might be deleted or modified by the attacker, causing irreversible changes to the contents or features of the application. In its worst case, an SQL injection attack may result in the compromise of a back end server or deteriorate the network infrastructure.

6. Phishing Attack: It is a category of social engineering wherein an attacker sends a deceitful message devised to trap a user into sharing sensitive information or deploying fraudulent software on the user device such as ransomware.

7. Password Attack: It occurs when a hacker tries to gain access to a user's password or steal it. Password attacks are prevalent in cases of poorly scripted passwords.

8. Brute Force Attack: It is a type of a commonly occurring attack in cryptography based on a cumbersome trial and error method employed by an attacker to acquire user credentials by desperately trying out all possible combinations of passwords, encryption keys. The attacker will try every possible passphrase until he cracks the right one.

9. DoS/DDoS Attacks: A denial-of-service (DoS) attack will usually flood a server with traffic, leading to unavailability of a website or resource whereas a distributed denial-of-service (DDoS) attack is a type of DoS attack which makes use of a multitude of computers or machines so that a targeted resource is flooded. Both these attacks will overload a server or web application intending to interrupt its routine services.

III. EXPLORING THE ROLE OF AI AND ML IN CYBERSECURITY

In recent years, AI and particularly ML have seen an unwavering demand and growth, also with their growing influence in all aspects of technology such as network security, cyber resilience, image and speech recognition, social media services to name a few. The tremendous growth has been a stimulus for heralding advancements in myriad fields and domains amongst which cybersecurity is the latest addition.

AI is but an extension of computer science that empowers machines with the ability to mimic human intelligence and natural brilliance. Devices and systems that employ AI features are capable of automating numerous mundane tasks and overcome shortcomings related to difficulty and complexity of those tasks which would be a manually impossible feat. This aspect of AI makes systems cognitive.

As cyberspace evolves, so does the risk of malware and cyberattacks. Not only are they strenuous to detect with standard procedures of cybersecurity, they also require laborious prevention and elimination techniques.

Such a scenario calls for an intelligent strategy to identify, analyse and eradicate possible cyber threats with efficacy. ML stands out as a trivial solution in this case, by promising better security from attacks by relying on data obtained from past attacks to combat new ones with a better competence and planning.

A noteworthy benefit of AI powered devices in cybersecurity apart from automation is the drastic reduction of manual involvement time from hundreds of hours to few seconds in the IT sector. Hence, AI and ML are utilised in conjugation to develop systems capable of tackling cyberattacks systematically without human intervention. [11] (Geluvaraj. B et al., 2019) Moreover, AI is also being deployed in cybersecurity applications to develop tools for pattern matching that can alert security analysts about any network issues and also equip the tools to offer real time response. It is unfortunate that cybersecurity being a constantly evolving, dynamic field demand that AI must also be capable of learning new analyst tactics, devise new strategies, learn from its failures and be armed with indomitable defence mechanisms. This enunciates the need for training sets to be created to foster research on cybersecurity so that unique AI tools for cyber analysts can emerge on par with rising threats.[12] (Bresniker et al., 2019)

IV. IMPACT OF AI AND ML

Trivially, AI and ML will aid in subsiding some threats like phishing at the noise level. However, as the scope of application expands, the prominence of AI and ML will be evident. They will help in early detection of DDoS attacks while preventing anomalies such as data leakage and intervention of private networks. By cumulative collection of training data for AI and ML methods, the industrial, academic sectors worldwide will be able to reap the benefit of establishing higher degree of cybersecurity.Systems that utilise AI principles are found to be helpful in automation of numerous tasks along with gearing up to complex and exhaustive situations much better than humans.

The newly emerging malware and cyber threats might pose difficulty in being detected using traditional approaches. Moreover since they keep evolving with time, it calls for more strenuous and vigorous approaches of detection. The solution to this issue relies on ML which uses patterns and data from previous attacks to respond to new ones. A second merit of using AI in cybersecurity is that AI equipped systems can reduce the time drastically for IT employees, while detecting threats. Such systems are devised to dynamically respond to any situation by itself. Most importantly, AI systems are error-free while handling tasks. This ensures that each attack is handled in an effective and practical manner.

When it comes to the combination of AI and cybersecurity, a vast range of interdisciplinary intersections comes into picture. AI technologies like deep learning can be incorporated into cybersecurity to tackle malware classification and intrusion detection by developing smart models.[13] (Li et al., 2018)

In order to combat today's cybersecurity issues, AI techniques that involve ML and DL have been the precursors along with the concepts of Natural Language Processing (NLP) ,Knowledge Representation and Reasoning (KRR) and rule-based Expert Systems (ES) playing a vital role. [14] (Sarker et al., 2021)

The AI techniques when employed for cybersecurity will offer advances in speed accuracy of performance, thus allowing autonomous action, reaction and defence to any kind of attacks by an adversary. [15] (Soni et al., 2020)

Having discussed the types of possible cyber attacks and the relevance of AI and ML in tackling them, it is now crucial to elaborate on the various algorithms and techniques of Machine Learning and discover their application in detecting some of the cyber and network threats. The table given below summarizes some of the most common Machine Learning techniques and their domains of relevance in the field of network and cyber security.

Table- I: An overview of various ML techniques and their relevance in the field of cybersecurity

ML Technique	Area/Domain of Relevance
Adaptive Boosting	In detecting network anomalies
Clustering	In analysing network intrusion detection
Decision Tree	• Analysing malicious behaviour • Modelling of anomaly detection and intrusion detection systems
Genetic Algorithm	• In intrusion detection systems • Prevention of cyberterrorism
Hidden Markov Model	In intrusion detection systems
K-Nearest Neighbour	Used to decrease the false alarm rate in network intrusion detection systems
Naive Bayes	In intrusion detection systems
Neural Network and Deep Learning	The RNN, LSTM and CNN techniques find profound use in : • Malware traffic classification, • Attack analysis • Anomaly intrusion detection
Random Forest	In network intrusion detection systems
Reinforcement Learning	To detect malicious activities and intrusions
Support Vector Machine	• In classification of attacks • Intrusion detection • Anomaly detection • DDoS detection and analysis

A. Network Anomaly Detection

A network anomaly describes an unexpected and short-term deviation from a network's normal operation. Some anomalies are intentionally caused by adversaries such as a denial-of-service attack (DDoS) in an IP network, whilst some may be accidental. The design of an efficient anomaly detection system demands sourcing of data from a vast and voluminous dataset with high-dimensions and noise. Various anomalies manifest themselves in different ways, which makes development of generalized models of network behaviour and also anomaly detection quite difficult. In [16], the authors (Yuan et al., 2016) have proposed a new method for network anomaly detection based on using a tri-training approach in combination with Adaboost algorithms. Adaboost, being one of the popular ensemble-based boosting technique, has been widely in use for improving the anomaly-based detection system accuracy. The term tri-training approach describes that three types of Adaboost methods, namely the Real, Discrete and Gentle methods were used in congregation. The tri-training approach proposed by the authors brings together the ideals of ensemble-based approach and the semi-supervised learning technique of ML. It thereby helps in minimizing the scope for errors and also offers higher efficacy and accuracy of anomaly detection. One of the powerful defence mechanisms against anomaly attacks happens to be fast detection. So as to develop an anomaly detection contrivance, the authors have worked on a semi-supervised Adaboost algorithm with specialities such as high precision, low time, low cost and low false-alarm rate. In the last few years, various anomaly detection techniques based on neural networks, support vector machine have been in use with a primary aim to classify user behaviour and activity as normal or abnormal. Generally, the techniques for anomaly detection can be broadly categorized into two types namely generative and discriminative. The generative method as described in [17] (Xueqin Zhang et al., 2006) tends to develop models purely on the basis of normal (no attack) examples used for training and later on evaluating every test case to check if it will fit the model or not. On the other hand, the discriminative method as discussed in [18] (C.Warrender et al., 1999) seeks to discern the difference between abnormal and normal cases/scenarios. Hence the model built using a discriminative approach will be trained using normal as well as abnormal (attack) examples. Authors (Hu et al., 2003) in their paper [19] have presented a novel approach for anomaly detection on the basis of robust support vector machines (RSVMs).While standard Support Vector Machine (SVM) can also be used, the authors have found that RSVMs have a notably lesser number of support vectors in comparison to standard SVMs. Moreover, RSVMs can also work with noisy data. The key intention of using RSVM is to be able to obtain a distinctively clear hyperplane to maximize the margin of separation between normal and anomalous network behaviour. The authors have tested the RSVM with a noisy dataset and analysed its robustness and performance of anomaly detection using Receiver Operating Characteristic (ROC) curve.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

B. Network Anomaly Detection

Network intrusion detection involves the identification of any spiteful actions that are aimed to falter and compromise some of the security measures and breach of integrity, confidentiality and availability of resources as a consequence.

In paper [20], the authors (Bama et al., 2011) have described a system capable of detecting network intrusion by utilizing the clustering concept. Clustering is a type of unsupervised learning method that groups together behaviours based on similarities. The various attacks or attempts of intrusion are treated as outliers. The authors have proposed a clustering technique using data mining intended to minimise false alarm rates and improvise the security.

Intrusion Detection Systems (IDS) are used to safeguard devices and systems housing crucial information against unforeseen intrusions and malicious attacks and to bridge any kinds of security gaps present in network access controls or operating systems.

The algorithm described by the authors aims to detect outliers that have been shared by a network to detect an intrusion. The outliers may sometimes form small clusters in which case, the aim is to utilise and compare outliers from various systems of the network if they are having identical similarity measure. If at least two systems on the network have outliers with the same similarity measure, then, it will indicate an intrusion attack which once detected, will enable a network administrator to set up a secure network. The algorithm once applied will be slated to perform a clustering task on patterns of usage of each site and detect common outliers. The elementary step to perform clustering is to identify the similarity between observed patterns. The degree of similarity will permit the grouping of normal patterns distinctively from the intrusion patterns. Consequently, the algorithm also performs clustering successively for each site, while keeping a check for possibly matched outliers.

Author S.Shilpashree, 2019 in paper [21] has explored how Decision Tree classifiers can be used to prevent network intrusion detection. Decision tree is capable of scrutinizing information and distinguishing those features of a system that demonstrate malicious activities. This helps in uplifting the security framework(s) as it checks the way in which the intrusion identification details have been arranged. It can decipher patterns and facilitates checking of known attack signatures. The Decision Tree classifier adheres to a vast set of straightforward rules that can be incorporated with real-time technologies easily.

A decision tree can be built to serve the process of validating incoming traffic, relying on a dataset to entitle grouping of new cases accurately. Presently, the author has considered a Classification and Regression Tree(CART) for intrusion detection amongst the many available methods to construct the decision tree. A classification and identification of four types of intrusion attacks namely DOS, R2L, U2R and Probing attacks has been tested by the author while comparing the performance of CART against Naive Bayes.

Authors (Wei Li, 2004) in their paper [22] have illustrated how the Genetic Algorithm (GA) can be used to tackle network intrusion detection. A genetic algorithm is regarded as a collection of computational models developed on the basis of natural selection as well as evolution. These set of algorithms will transform the problem from one particular domain into a model by utilising a data structure similar to chromosomes. This genetic algorithm can be applied to develop uncomplicated rules for the network traffic, which shall aid in distinguishing between normal and anomalous network connections. An anomalous network connection indicates the vulnerability to a probable intrusion attack. The genetic algorithm can be initiated with a handful of generated rules and it can progressively generate a expansive set of rules for IDS. These rules serve to filter network traffic efficiently. The main aim while using Genetic Algorithm is to improve the detection rate while also trying to minimise the false positive rate. This has been reinstated by authors (S. E. Benaicha et al., 2014) in paper [23]. Authors of [24] (Yin et al., 2003), have shown that network intrusion can be predicted using a Hidden Markov Model (HMM). A HMM is a statistical Markov Model which assumes the system that is being modelled as a Markov Process. It is a two tier stochastic process with an unobservable stochastic process at the first tier. The HMM is helpful for modelling sequence information. The authors talk about a novel approach utilising HMM to detect signature based intrusion attacks. The attack signatures are a testament to intrusive or malicious activity or traffic. A HMM model is used to analyse network traffic at both the source and destination and was proven to have reduces false positive rate. Usually, the standard HMM will have a fixed number of states which must be decided upon beforehand. The authors have experimentally found that the HMM model works best with 4 to 16 number of states. They have compared the false positive rate and detection rate for 5, 10 and 16 states respectively. Authors (Panda et al., 2007) in their paper [25] , have discussed utilising the Naïve Bayes method for an intrusion detection system. The Naive Bayes classifier is based on the Bayesian Classification whose hypotheses articulates that provided data belongs to a specific class. The probability of the hypotheses being true will be evaluated. This serves as a very practical approach. The framework for network intrusion detection based on Naive Bayes algorithm will effectively build patterns of a network's services over a data set that has been labelled by the services of the network. These patterns help the framework in detecting the intrusion attacks. The authors have analysed the performance of the Naive Bayes method by employing it to detect probing attack, Denial of Service attack, U2R attack and R2L attack and compared the precision of the detection and false positive rate for each of these attacks. In the paper [26] (Liao et al., 2002), it has been depicted that intrusion attacks can be detected and avoided by employing a novel technique that is based on k-Nearest Neighbour classifier (kNN). This elementary machine learning classifier has been deployed to learn program behaviour to perform intrusion detection. The k-Nearest Neighbour (kNN) classifier has proven to be successful in classifying program behaviour as being intrusive or normal in case of text categorization applications. Basically, text categorization deals with the content-based grouping of textual data into one or many classes.

This employs techniques of machine learning such as support vector machine, decision tree, regression model as well as statistical classification. The primary task in text organization is the transformation of textual data in the form of character strings into a form that is apt for the learning algorithm being used for classification. In this case, the vector space model comes in handy. Text categorization will accordingly convert every process into a vector. The authors also assert that the kNN technique has been found effective in detecting intrusion and helping to achieve quite low false positive rates. In comparison to other known methods, the kNN classifier does not require learning of and distinct program files due to which the computation involved in classification of any program behaviour is significantly reduced. The authors have evaluated the kNN classifier performance by considering a value of 10 for k and choosing a threshold of 0.8. The performance metrics computed were the prediction accuracy and false positive rate. In their paper [27], authors (Zhang et al., 2008) have outlined a technique that uses Random Forest algorithm for intrusion detection in three aspects namely for misuse detection, anomaly detection and hybrid detection. In case of misuse detection, all possible patterns of probable or occurred intrusions are automatically generated by the random forest algorithm from the data provided for training. Once that is done, intrusion detection is accomplished by comparing and finding matches between network activity and previously known patterns. In consequence of anomaly detection, the outlier detection technique of random forest algorithm helps in intrusion detection. Once the network service pattern(s) have been developed, the outlier detection method will identify network intrusions by virtue of the outliers that are found to be related to the known patterns. When in case of hybrid detection, there is an improvement in the efficacy of detection because it is an amalgamation of both the anomaly detection and misuse detection techniques. The advantage of using Random Forest algorithm in rule-based systems lies in the fact that it can impulsively build patterns by learning from training data in an automatic manner without the need for manual coding of any rules. In paper [28] authored by (K.Sethi et al., 2020), there has been a proposition to inculcate Deep Reinforcement Learning (DRL) adaptive method for Intrusion Detection. The authors opine that though there have evolved many machine learning based techniques for intrusion detection, yet these methods perform poorly when large datasets are employed and multiple classifications are involved. The existing methods need to be represented using high dimensions. This shortcoming was resolved by resorting to Deep Learning (DL), which happens to be an advanced technique. It is capable of learning feature representation at various granularity levels from the data fed as input using a deep hierarchical framework. There have been advancements in this aspect leading to a handful of solutions for intrusion detection using deep neural networks, and recurrent neural networks. Talking of Reinforcement Learning (RL), it is a simple framework to learn decision-making in a sequential manner. Of Late, deep reinforcement learning (DRL) that is essentially a combination of reinforcement learning and deep learning has emerged that has been found to be beneficial for intrusion detection. The DRL technique combines two DL based models namely a binomial classification model to indicate an intrusion attempt and a multinomial model in order to find out the category of the intrusive attack. Authors (Mulay et al., 2010), in their paper [29] have shown through elaborate studies and discussion as to how the Support Vector Machine classifier can be utilised for classifying intrusion attacks. SVM evades complexity in computation by using a kernel function. Usually, SVM classifier performs binary classification, and goes by the name of Binary SVM. The authors have proposed combining the Binary VMs along with decision trees leading to multiclass SVMs in order to aptly distinguish various network attacks such as DoS and DDoS and also cater to anomaly detection. The multiclass SVM will create 'k' number of distinct classes during the training phase of intrusion detection.

Table- II: A comparative analysis of results offered by various ML algorithms for Network Intrusion Detection

Method Used	Performance Metrics and their Criteria		Results
	Metric	Criteria for metric	
Clustering	Execution Time	For 500 users For 1000 users For 1500 users For 2000 users	185 seconds 290 seconds 412 seconds 526 seconds
Decision Tree (CART)	Detection Rate	For Probing Attack For DoS Attack For U2R Attack For R2L Attack	99.52% 98.94% 99.65% 94.04%
Genetic Algorithm	Detection Rate False Positive Rate	- -	99.74% 3.74%
Hidden Markov Model	Detection Rate False Positive Rate	For 5 states For 10 states For 16 states	100% 0.436% 1.67% 1.45%
Naïve Bayes	Detection Rate False Positive Rate	For Probing Attack For DoS Attack For U2R Attack For R2L Attack For Probing Attack For DoS Attack For U2R Attack For R2L Attack	96% 99% 90.47% 90% 0.0014% 0.26% 0.000163% 0.00025%
k-Nearest Neighbour	Detection Rate False Positive Rate	- -	91.7% 0.59%
Random Forest	Execution time	Without feature selection With feature selection	491 seconds 423 seconds
Deep Reinforcement Learning	Detection Rate False Positive Rate	- -	83.8% 2.6%
Support Vector Machine	Validation accuracy Classification accuracy	- -	89.85% 99.9%

The problem of anomaly detection falls in the category of a classification problem essentially. The aim of anomaly detection is the separation of normal data from anomalous data. In paper [30] by (S. Mukkamala et al., 2002), the authors have carried out anomaly detection using SVM. The registry activity of a system's operating system was used as the basis for the SVM to classify accesses to that system as normal or attack oriented.

SVM can also be employed for classifying network attacks because SVM fundamentally finds a decision surface in vector space that serves to separate data vectors into two classes. The SVM classifier can classify various attacks to the class which they belong and in case the attack is classified properly it gives a “yes” result and a “no” result in case the predicted attack is not the same as the occurred attack. The same claim has been supported in paper [31] by (Kotpalliwar et al., 2015).

V. RESULTS AND DISCUSSION

With regard to the comparison depicted in Table 2, we discern that the performance of an ML algorithm in detecting network intrusion relies on certain factors namely the execution time, the detection percentage, the false positive rate. But in the case of the Support Vector Machine algorithm, the performance depends on the validation accuracy and classification accuracy.

Amongst the various algorithms, it is observed that the highest detection rate of 100% for all kinds of network intrusions is offered by the Hidden Markov Model. This model has been equipped to detect a plethora of abnormal network behaviours and not constrained to the detection of certain predefined and suspected intrusion attacks.

On the other hand, the Genetic Algorithm offers a detection rate of 99.74% and is therefore the second best choice for intrusion detection. Next, the k-Nearest Neighbour classifier offers a detection rate of 91.7%, making it the third best choice. Lastly, the Deep Reinforcement Learning method offers a detection rate of 83.8% which is lesser compared to previous techniques.

In the case of the Naive Bayes method and Decision Tree method , it is to be noted that these models are trained and tested to specifically detect the Probing attack, DoS attack, U2R attack and R2L attack. The Decision Tree based intrusion detection model is advantageous owing to its high detection rates namely 99.52% for the probing attack, 98.94% for the DoS attack, 99.65% for the U2R attack and 94.04% for the R2L attack respectively whereas the Naive Bayes based intrusion detection model offers detection rates of 96% for the probing attack, 99% for the DoS attack, 90.47% for the U2R attack and 90% for the R2L attack respectively.

Certain ML techniques such as the clustering approach and Random Forest approach are compared and evaluated based on their execution time in order to perform intrusion detection. The execution time of the model based on the clustering method is a variable parameter that depends on the number of users on the network. When there are more users on a network, the time taken for execution increases invariably.

Most methods are also tested to examine their false positive rate. The false positive rate is a measure of the false positive states identified by an intrusion detection system. Every technique will offer different false positive rates. The lesser the false positive rate, the better the performance.

VI. CONCLUSION

From the discussed prospects we find that Artificial Intelligence and Machine Learning play a significant role in simplification and rationalization of cybersecurity approaches to handle cyber attacks such as network intrusion. Machine Learning serves as a luminary of algorithms that can be employed to detect network intrusions and anomalies. The field of Machine Learning has offered an array of beneficial applications in the development of novel cybersecurity techniques. It has been helpful in the alleviation of some common shortcomings of earlier cybersecurity methods such as low detection rate and high false positive rate. Furthermore, as the networking and cyber sector is witnessing manifold progress and growth, the scope for implementing highly potent and efficient systems for threat detection is very high, the idea of utilizing Machine Learning algorithms is opportune. Future scope in the field of cybersecurity lies in employing techniques such as cloud computing, quantum computing, dynamic networks and predictive semantics to thwart cyber threats.

REFERENCES

1. Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21. http://doi.org/10.22215/timreview/835 [CrossRef]
2. R. A. Kemmerer, "Cybersecurity," 25th International Conference on Software Engineering, 2003. Proceedings., 2003, pp. 705-715, doi: 10.1109/ICSE.2003.1201257. [CrossRef]
3. Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." Journal of Computer and System Sciences 80.5 (2014): 973-993. [CrossRef]
4. Symantec Security Summary 2020. [online] https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-june-2020 (Accessed 21st September 2021)
5. Cyber Security Report 2020 [online]https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf (Accessed 25th September 2021)
6. Bendovschi, Andreea. "Cyber-attacks–trends, patterns and security countermeasures." Procedia Economics and Finance 28 (2015): 24-31. [CrossRef]
7. Biju, Jibi Mariam, Neethu Gopal, and Anju J. Prakash. "Cyber attacks and its different types." International Research Journal of Engineering and Technology 6.3 (2019): 4849-4852.
8. Fischer, Eric A. "Cybersecurity issues and challenges: In brief." (2014).
9. Hussain, Abdulla, Azlinah Mohamed, and Suriyati Razali. "A Review on Cybersecurity: Challenges & Emerging Threats." Proceedings of the 3rd International Conference on Networking, Information Systems & Security. 2020. [CrossRef]
10. Pogrebna, Ganna, and Mark Skilton. "Cybersecurity Threats: Past and Present." Navigating New Cyber Risks. Palgrave Macmillan, Cham, 2019. 13-29. [CrossRef]
11. Geluvaraj, B., P. M. Satwik, and TA Ashok Kumar. "The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace." International Conference on Computer Networks and Communication Technologies. Springer, Singapore, 2019. [CrossRef]
12. Bresniker, Kirk, et al. "Grand challenge: Applying artificial intelligence and machine learning to cybersecurity." Computer 52.12 (2019): 45-52. [CrossRef]
13. Li, Jian-hua. "Cyber security meets artificial intelligence: a survey." Frontiers of Information Technology & Electronic Engineering 19.12 (2018): 1462-1474. [CrossRef]

14. Sarker, Iqbal H., Md Hasan Furhad, and Raza Nowrozy. "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions." SN Computer Science 2.3 (2021): 1-18. [CrossRef]
15. Soni, Vishal Dineshkumar. "Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA." Available at SSRN 3624487 (2020). [CrossRef]
16. Yuan, Yali & Kaklamanos, Georgios & Hogrefe, Dieter. (2016). A Novel Semi-Supervised Adaboost Technique for Network Anomaly Detection. 111-114. 10.1145/2988287.2989177. [CrossRef]
17. Xueqin Zhang, Chunhua Gu and Jiajun Lin, "Support Vector Machines for Anomaly Detection," 2006 6th World Congress on Intelligent Control and Automation, 2006, pp. 2594-2598, doi: 10.1109/WCICA.2006.1712831. [CrossRef]
18. C. Warrender, S. Forrest and B. Pearlmutter. “Detecting Intrusions Using System Calls: Alternative Data Models.” In Proceedings of 1999 IEEE Symposium on Security and Privacy, pp 133-145, Oakland, 1999.
19. Hu, Wenjie & Liao, Yihua & Vemuri, Rao. (2003). Robust Anomaly Detection Using Support Vector Machines. Proceedings of the International Conference on Machine Learning.
20. Bama, S. Sathya, Irfan Uddin Ahmed and Hindusthan. “Network Intrusion Detection using Clustering: A Data Mining Approach.” International Journal of Computer Applications 30 (2011): 14-17.
21. S., Shilpashree. (2019). Decision Tree: A Machine Learning for Intrusion Detection. International Journal of Innovative Technology and Exploring Engineering. 8. 5. 10.35940/ijitee.F1234.0486S419. [CrossRef]
22. Li, Wei. (2004). Using genetic algorithm for network intrusion detection.
23. S. E. Benaicha, L. Saoudi, S. E. B. Guermeche and O. Lounis, "Intrusion detection system using genetic algorithm," 2014 Science and Information Conference, 2014, pp. 564-568, doi: 10.1109/SAI.2014.6918242. [CrossRef]
24. Yin, Qingbo & Shen, Li-Ran & Zhang, Ru-Bo & Li, Xue-Yao & Wang, Hui-Qiang. (2003). Intrusion detection based on hidden Markov model. 10.1109/ICMLC.2003.1260114.
25. Panda, Mrutyunjaya & Patra, Manas. (2007). Network intrusion detection using naive bayes. 7.
26. Liao, Yihua & Vemuri, Rao. (2002). Use of K-Nearest Neighbor classifier for intrusion detection. Computers & Security. 21. 439-448. 10.1016/S0167-4048(02)00514-X. [CrossRef]
27. Zhang, Jiong & Zulkernine, Mohammad & Haque, A.. (2008). Random-Forests-Based Network Intrusion Detection Systems. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on. 38. 649 - 659. 10.1109/TSMCC.2008.923876. [CrossRef]
28. K. Sethi, R. Kumar, N. Prajapati and P. Bera, "Deep Reinforcement Learning based Intrusion Detection System for Cloud Infrastructure," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020, pp. 1-6, doi: 10.1109/COMSNETS48256.2020.9027452. [CrossRef]
29. Mulay, Snehal & Devale, P.R. & Garje, Goraksh. (2010). Intrusion Detection System Using Support Vector
30. Machine and Decision Tree. International Journal of Computer Applications. 3. 10.5120/758-993.
31. S. Mukkamala, G. I. Janoski, and A. H. Sung. “Intrusion Detection Using Support Vector Machines”, Proceedings of the High Performance Computing Symposium - HPC 2002, pp 178-183, San Diego, April 2002.
32. Kotpalliwar, Manjiri & Wajgi, Rakhi. (2015). Classification of Attacks Using Support Vector Machine (SVM) on KDDCUP'99 IDS Database. 987-990. 10.1109/CSNT.2015.185. [CrossRef]

AUTHORS PROFILE

Swathi Dayanand, is currently working as a Security Network Consulting Engineer 1 at Aryaka Networks. She has completed her B.E., in ECE from BNM Institute of Technology, Bangalore. She has also been awarded the ‘Best Outgoing Student’ post completion of her B.E., course. She is the VTU State Topper for ECE and has been felicitated with 7 Gold Medals by VTU. She has published two papers previously in reputed International Journals.

Dr. Chaitra N, currently working as an Associate professor in the Department of Electronics and Communication Engineering, BNM Institute of Technology has around 15 years of experience in teaching and industry together. She did her B.E from BMS College of Engineering and Master’s from RV College of Engineering, Bangalore. She was a topper for her branch in both under and post-graduation studies and received Gold medal from VTU for securing first rank in M.Tech. She completed her Ph.D under VTU in the area of image processing, machine learning and pattern classification.

She was working as Software Engineer at Infosys Technologies Ltd.,before joining BNMIT as a lecturer. She has over 18 publications in reputed international journals and conferences. She has also filed two Indian patents and one of them is published. She has received “Best Faculty award” from Cognizant Technologies for the year 2014-15.