An IDS For SDN-Based Networks Using Machine Learning Techniques To Identify Network Attacks

G.Venkateswara Rao[1], Dr. Rajeev Yadav[2], Dr.G Syam Prasad[3]

[1]*Research Scholar, Dept.of CSE, SKU,* Chhatarpur, Madhya Pradesh*, India.*
[1]*gvraocse777@gmail.com*

[2]*Professor, Dept.of CSE, SKU,* Chhatarpur, Madhya Pradesh*, India.*
[2]*rajeevyadav@gmail.com*
[3]*Professor& HOD, Dept.of IT, Narasaraopeta Engineering College, Guntur, A.P, India.*
[3]*syamprasad.gudapati@gmail.com*

Abstract

Software Defined Networking Technology (SDN) provides a prospect to effectively detect and monitor network security problems ascribing to the emergence of programmable features. Recently, Machine Learning (ML) approaches have been implemented in SDN-based Network Intrusion Detection Systems (NIDS) to protect computer networks and overcome network security issues. A stream of advanced machine learning approaches –deep learning technology (DL) commences emerging in the SDN context. In this survey, we reviewed various recent works on machine learning (ML) methods that leverage SDN to implement NIDS. More specifically, we evaluated the techniques of deep learning in developing SDN-based NIDS. In the meantime, in this survey, we covered tools that can be used to develop NIDS models in an SDN environment. This survey is concluded with a discussion of ongoing challenges in implementing NIDS using ML/DL and future works.

Keywords: *NIDS, Machine learning, Network security,Types Attacks, SDN*

1. Introduction

Network Intrusion Detection systems (NIDS) have been developed rapidly in academia and industry in response to the increasing cyber-attacks against governments and commercial enterprises globally. The annual cost of cybercrime is continuously rising. The most devastating cybercrimes are those caused by malicious insiders, denial of services, and web-based attacks. Organizations can lose their intellectual property with such malicious software crept into the system which may lead to disruptions to a country's critical national infrastructure. Organizations deploy a firewall, antivirus software, and an intrusion detection system (NIDS) to secure computer systems from unauthorized access [1]. One of the focused areas to resolve cyber-attacks quickly is to detect the attack process early from the network using NIDS. Network intrusion detection systems (NIDS) are designed to detect malicious activities including viruses, worms, and DDoS attacks. The critical success factors for NIDS are abnormality detection speed, accuracy, and reliability. Machine learning techniques (ML) are applied to develop NIDS to improve detection accuracy [2] and low false alarm rates. As an advanced stream of ML, deep learning (DL) approaches have been adopted in the field of NIDS. The recent development focuses on leveraging a new network architecture, namely, the software-defined network (SDN) to implement NID with machine learning approaches. The software-defined network is an emerging architecture that decouples the network control and forwarding functions so that the network control can be directly programmable. The segregation of the control plane from the data plane enables easy network management. This feature of SDN is facilitating innovative applications, dictating a new networking paradigm capable of implementing NIDS. Machine learning and deep learning (ML/DL) approaches can be implemented in the SDN controllers to enhance network monitoring and security. Several research works have been done to implement NIDS, with integrated deep learning algorithms using SDN controllers before. In [3], the authors integrated an anomaly algorithm into open-flow switches using a controller. They constructed a deep neural network to simplify the features of normal and abnormal traffic. To evaluate their model, they also implemented deep learning algorithms. An SDN-based DDoS detection system comprised of three modules. The three modules are implemented on the top of the controller and a deep learning approach was used for feature extractor and traffic classification. A lightweight DDoS flooding attack detection solution, which uses emulation to build a NOX-based network in SDN using a self-organized map (SOM). There are many review papers covering ML/DL methods in various domains. Little has been done around NIDS based on SDN. We focus on depicting SDN as a platform for implementing NIDS with ML/DL approaches beyond the reach of existing review works.

2. Software Define Network (SDN)

The existing network devices such as routers and switches have operating systems that have a limited set of configuration options. If network administrators or security engineers what to make significant changes by deploying new protocols or technologies which are not currently supported, they must change the whole device must be changed which is a costly and unacceptable approach.

The concept of Software Define Network (SDN) involves managing network services through the abstraction of lower-level functionality. In other words, the separation of data and control planes with a well-defined Application Programmable Interface (API) is the main characteristic of SDN. Data plane functionalities cover all activities related to data packet transmitting, such as forwarding, fragmentation, reassembly, replicating for multicasting, etc.

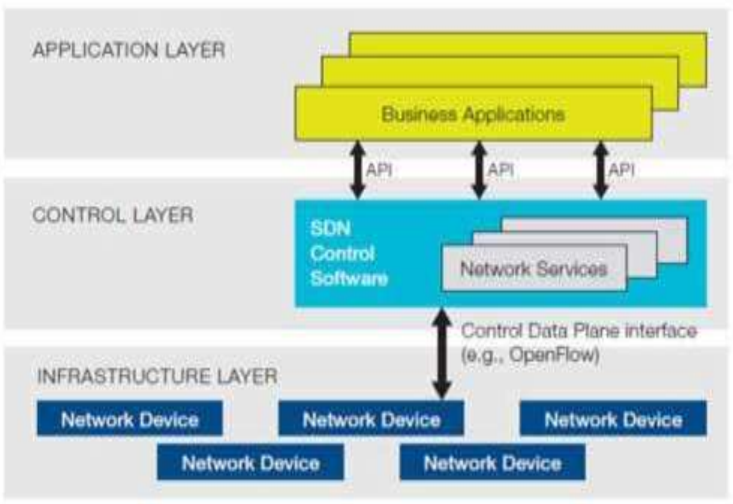

Figure 1. Software-Defined Network Architecture [1]

The Control plane defines functional logic for network communication equipment (routers or switches) that determines how one device communicates with other devices in the network. All the routing protocols in routers or other protocols with switches are control plane protocols. It includes all activities that are necessary to operate the data plane, but do not involve end-user data packets (making routing tables, setting packet handling policies, base station beacons announcing the availability of services). Figure 1 depicts a logical view of the SDN architecture. Network intelligence is (logically) centralized in software-based SDN controllers, which maintain a global view of the network [4]. Open Flow Protocol (OPF) is a programmable network protocol that is designed to manage the traffic in SDN network. OpenFlow Protocol is the first standard communications interface defined between the controllers and forwarding layers of SDN architecture. It is a programmable open protocol designed to direct and manage communication between network devices and the central network controller.

2.1. Intrusion Detection System (IDS)

The Intrusion Detection System (IDS) is software or hardware that is used by system administrators and security engineers to monitor the characteristic of a single host or monitor and analyses the whole network traffic to distinguish between legitimate and attacks traffic. In case of attacks, it generates alarms to keep track of malicious activities [5].

2.1.1. Types of attackers

The following types of attackers are recognized and classified in the literature.

- **Masquerade**
  An individual who is not authorized to use the computer and who penetrates system access control to exploit legitimate user accounts. It’s likely to be an outsider.
- **Midseason**
  There are two subtypes of attackers: one is a legitimate user with no permission to access an application, while the other is a legitimate user who misuses the privileges. Both of them are likely to be insiders.
- **Clandestine user**
  An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. It could be either insider or an outsider.

2.1.2. Types of Intrusion Detection Systems

Intrusion Detection Systems can be categorized based on what they target into the following :

- **Host-based Intrusion Detection System (HIDS)**
  It is a special software on a computer that monitors what happens in that computer, with the aim of detecting is there someone intruding or not.
- **Distributed host-based Intrusion Detection System (DHIDS)**

Intrusion detection software is distributed on many computers or special devices, monitoring malicious activities. They often report back to some other central computer to improve the chance of detecting intrusions.

- **A network-based Intrusion Detection System (NIDS)**
  Inspects network traffic to identify suspicious activity by monitoring network traffic behaviour at different points across the network and correlating this information they can recognize anomalies in traffic patterns. The analysis may be done in the sensors or may be sent information back to the management server that analyses all of them.
- **Wireless Intrusion Detection System (WIDS)**
  It uses to monitor the wireless LAN using sensors distributed in a wide physical network detection placement within a range of existing wireless signals.

2.1.3. Common components

The main components that are used in almost every intrusion detection system are [7]:

- **Sensors:** collect data, e.g. packets using TCP-dump or Wireshark, log files (concerning applications), and system call traces (concerning the operating system).
- **Analyser:** received collected data, analyse it and determine if intrusion.
- **User interface:** allow security experts, system administrators, and other users to view the output and control behaviour of IDS.

3. Network security Applications

3.1. Intrusion detection

An intrusion detection system (IDS) has been developed that’s capable of detecting every kind of network attack within the environment. IDS detects malicious network activities by analyzing the collected packets, and alarms to the computer user, and blocks attack connections from attacks [8]. It additionally connects with the firewall as an elementary technology for network security. The characteristics of the network are being assessed into Host-based intrusion detection (HIDS) which involves inputting packages and monitoring internal packets of the system. To perform intrusion detection HIDS gathers data from its system calls, OS audit trails, application logs, etc. Network-based intrusion detection which detects malicious activity in network traffic. Generally, intrusion detection algorithms unit classified into 2 methods: misuse detection (Signature-based) and anomaly detection. Signature-based IDS: It is a technique that looks at a series of bytes or sequences with a malicious network and helps track down the detailed log of the system which causes a false alarm. Anomaly-based IDS: It helps in identifying the anomalies and indicates serious and rare events over the system and rectifies the unusual traffic pattern in a network. To resolve the disadvantage of these two detection methods Hybrid IDS has been proposed which combines the complexity of anomaly and issue detection systems and gets with the new framework. Nowadays, the self-learning system becomes one of the prominent methods. Machine learning is one of the most powerful concepts. Most of the ML solutions resulted in achieving a high false positive rate and high machine computation. This is due to most machine learning techniques coming up with the learning patterns among small-scale, low-level feature patterns of traditional and attack connection records. Most notably machine learning comes with deep learning which will be outlined as a better model of machine learning algorithms. These will help in learning the representation techniques with highly advanced hierarchic sequences. The model for a novel deep learning approach in NIDS operation over networks, with a combination of deep and shallow learning methods [9]. This helps in the analysis of network traffic over the non-symmetric deep auto-encoder technique (NDAE). In [10] a brief study explains that Long short-term memory(LSTM), Recurrent neural network(RNN), and Convolution neural network(CNN) performs well in IDS systems when compared to other machine learning algorithms. CNN with the n-gram technique is briefly discussed along with hybrid networks such as CNN, CNN recurrent neural network (CNN-RNN), CNN-long short-term memory (CNNLSTM), and CNN-gated recurrent unit (GRU). These techniques help in the identification of good and bad network IDs in network connections. CNN can gain high-level feature representation from low-level feature sets during the extraction process is disused in [10]. Following with system call modeling based approach with ensemble method is proposed using LSTM algorithm for anomaly-based IDS system. System call modeling helps capture the semantic meaning of every call and relation over the network. Ensemble methods focus on false alarm rate which fits IDS design. This is a compact method, which helps in the storage of parameters in a small space. This method is considered a fast and efficient approach in sequential matrix applications [11-12].

3.2. Malware detection

Malware is programs that disrupt the data, and files in the system which reduces the vulnerability and performance. In some cases, it will lead to total corruption of the system or server. These are easily passed through various environments using unauthorized software tools. There are existing works in which deep learning has become one of the prominent methods in malware analysis. The binary and multi-classifier techniques are used for classification which gives better results when processed with rectified linear unit activation functions and dropout over the hidden networks. The deep learning approach applied with a four-layer network design is discussed. To get modest computation feature text extraction techniques such as Byte/Entropy Histogram Features, PE Import Features, String 2D histogram features; PE Metadata Features can be used. A brief discussion is made to show how to prevent overfitting and how the backpropagation method helps in speeding up the learning process over the network. The echo state networks (ESNs) and recurrent neural networks (RNNs) help in extracting full information by random temporal projection technique. Max pooling is used for non-linear sampling of data and logistic regression for the final classification of data. An advanced malware technique known as Ransomware. It is a kind of crypto viral extortion which helps encrypt files and gather information without other knowledge [13]. The deep learning algorithm LSTM is been applied to API calls by binary sequence classification method [14]. They evaluated the performance of classical machine learning classifiers and deep neural networks on malware detection.

3.3. Android malware detection

Android device has become popular nowadays among peoples. Malware detection becomes a big challenge in the android platforms. Deep learning along with NLP comes with a great breakthrough in this area [15] Droid detector is a Google app that helps collect malware data.

The collected data is processed for both static and dynamic analysis for feature extraction and it is characterized by DBN based approach. The semantic information extraction from the system call the sequence method using NLP which helps in the construction of a deep learning model [16]. The LSTM model is constructed with an effective number of hidden layers to achieve better results. The time cost function is used for classification by implementing different frameworks like Tensor flow to speed up the process. This model is being compared with the n-gram model which is considered a superior detection method for android malware. Hyper parametric tuning is being done in the LSTM network, and LSTM-RNN network topology explains how the architecture helps in getting better results. The effectiveness of the API call sequence is being studied, to perform this CNN is been approached by discussing the training size and sequence length which gives a better indication of the false and negative positive.

3.4. Domain name generation algorithms (DGAs)

Domain fluxing malware is possessed through a domain generation algorithm(DGA). This malware encodes through a domain or IP address by blocking the network from further communication between the server and the host [16]. A detailed study on DNS log collection and deep learning for detecting malicious domain names on large scale is discussed. The explains DNS logs in side LAN environment which use deep learning algorithms for the detection of malicious domain names and compared with the traditional machine learning algorithm. They claimed that the deep learning algorithms performed well in comparison to the traditional machine learning algorithms and these algorithms remain as robust in an adversarial environment. A detailed study of the statistical feature approach on DGA systems by splitting the features into domain length, and domain level using the n-gram technique. In this approach, the Hidden Markov model (HMM) is been used for classification. These traditional techniques are very slow and poor in the performance of false and true positives. The deep learning technique helps in the discrimination of DGA domains from non-DGA domains. In [17] focused mainly on Character-based methods using neural networks such as RNN, CNN, and Hybrid CNN. In RNN Endgame model is used which improves the model performance by adding dropout to overcome dropout during the training phase along with the embedding technique. To get better predictive accuracy CMU model is implemented along with Bidirectional RNN. The NYU and Invincea models are discussed with CNN and the hybrid architecture of CNN is explained along with the MIT model. All these models consist of multiple layers and are termed the most extensive architectures. The LSTM network comes up with the advantage of featureless extraction of raw domain names as an input is also discussed. proposed a unique framework that correlated the data of DNS, URL, and Email to increase malicious activities detection rate.

3.5. Spam and Phishing Detection

The study shows that spam email is the act of sending undesirable information or mass information in a substantial amount to some email accounts. It is a part of electronic spam including almost indistinguishable messages sent to different beneficiaries by email. Along with phishing other cyber-crime technique scams other personal information such as passwords, credit card details, bank accounts, etc. These problems are rectified using deep learning techniques with Natural language processing (NLP). The phishing techniques over mail using an unbalanced dataset. Mainly in this various techniques such as term frequency-inverse document frequency (TF-IDF), Nonnegative Matrix Factorization (NMF), and a bag of words are discussed for feature extraction, and also algorithms such as Random forest(RF), logistic regression, k-nearest neighbor, Multi nominal navies Bayes are used. LR and MLB come with high metric performance [18]. The neural network approach is discussed by applying pearl script for feature extraction which helps to get the dataset in a vector format. A comparative study is done on the extracted dataset using Traditional machine learning algorithms in which Decision tree (DT), and neural network approach performed well [19]. The NLP feature extraction techniques use methods such as character-level embedding and word embedding. A comparative study is made among Support vector machines (SVM) using character level and CNN using both character and word embedding techniques. CNN using word embedding gives a better result [20]. A new LSTM approach in which datasets are considered as a hierarchical email architecture by considering them as sentences and words. Bidirectional LSTM is used for both cases which helps in computing the weight and estimates the phishing probability over the data during the network computation [21]. The neural network is used for the classification of URL phishing it consists of a three-layer linear network which makes the topology very light and compact. Malicious threats over URLs is been analyzed by character sequence [22]. The embedding technique is used with RNN and hybrid CNN networks which helps in studying how to develop a shelter for web page content analysis from malicious URLs with faster web page response. The application of CNN is leveraged for image spam detection [23]. The application of CNN and CNN-LSTM for phishing URL detection and compared with bi-gram text representation [24].

3.6. Traffic Analysis

The density and the volume of internet traffic is being increasing day by day. Identification of data flow through the network is considered a major problem in traffic analysis [25]. The traditional method uses Artificial neural networks and deep learning methods and the result shows that in feature learning, and unknown protocol identification this approach is very well but it could give better adaptation in a non-automation method in the traditional method [26]. A deep packet framework for extracting features automatically from network traffic using the Deep learning method is proposed in these packets to help handle sophisticated tasks like multi-challenging, traffic, etc. An architecture for Shallow and deep networks for secure shell protocol [28]. which RNN network helps to classify and model the tunnel SSH by modeling the time series feature to identify statistical information of the traffic flow [29].

3.7. Binary Analysis

Binary analysis is a powerful security analysis tool that looks into binary codes and finds the vulnerability issues with uncertainty deploying in free and open software. Static analysis can understand the pattern of the code to find vulnerabilities. Nowadays automated analysis method is combined with the deep learning method which has overcome the pattern-based limitations. The different problems faced in binary analysis and how they can be solved using neural networks. Many benchmark approaches are analyzed with RNN, LSTM, and GRU networks. To rectify Gradient descent over the hidden layers, optimization is done with the

RMS proposed method. This is also being discussed with the background behind all networks with time function, error analysis, function identification, and limitation of the network. An RNN network but in this work, so many experiments are performed on machine code snippets. These snippets are performed on LLVM and MIPS binaries data using a tokenization scheme. These help in the extraction of higher-level structures from lower-level binary structures. A new system EKLAVYA helps in recovering function type signatures from disassembled binary codes using the RNN network. The argument recovery module on RNN is implemented using techniques like saliency mapping and sanitization. This system helps in learning calling conventions and idioms with high-level accuracy parameters [30]. The deep learning method on assembly codes helps to analyze the software's weaknesses. In this TextCNN is been analyzed using Instruction2vec and word2vec which has given high accuracy in the classification of text data.

4. Intrusion Detection Methods

The source of data that is analyzed by the IDS is either whole packet data, which is the transitional IDS used to inspect the whole payload, or flow-based IDS which only takes basic accounting information of the communication in the network (header of the packet, number of bytes and packets in both directions). Therefore, flow-based IDS reduces the amount of data to be analysed, which makes them especially interested in SDN-based systems. IDS use a variety of detection and analyses methods to evaluate the traffic crossing the network, and can be categorized based on how they identify intrusion into the following:

- Signature-based detection (Packet-based) Known as knowledge-based or misuse-detection it defines the behaviour or attacks by a set of rules or patterns; compares observed behaviour against these rules/patterns. Usually, techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. This method is widely used because many attacks have clear and distinct signatures [31].
- Rule-based anomaly detection: define rules based on past observed normal behaviour. It also involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behaviour is that of an intruder.
- Rule-based penetration identification: define rules based on attacks. Typically, the rules used in these systems are specific to the machine and operating system, the most fruitful approach to developing such rules is to analyse attack tools and scripts collected on the internet. These rules can be supplemented with rules generated by knowledgeable security personnel.

It is used for the expert intelligent system that tries to analyse the user packets and from that analysis the classification between legitimate and illegal users is made. The problem with this approach is that a new attack cannot be detected either because the database is out of date or the signature is not available yet. Another weakness is the time taken since it supposes to compare all the signatures. However, it achieves high accuracy with a low number of false alarms [32]

- Anomaly-based Detection (Flow-based) Known as statistical anomaly-based, behaviour-based, or baselining, it involves the collection of data relating to the behaviour of legitimate users over some time. Statistical tests are applied to observed behaviour to determine whether it is a legitimate user or not. There are two types:

- Threshold detection: threshold based on the frequency of occurrence of events, independent of the user. It involves counting the number of occurrences of a specific event type over an interval of time. If the count surpasses what is considered a reasonable number that one might expect to occur, then intrusion is assumed. By itself is a crude and ineffective detector of even moderately sophisticated attacks.
- Profile-based: A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts [33].

The advantages of this technique are the ability to detect new types of attacks. It has the disadvantages which require more overhead, and processing capacity, and producing a false alarm.

4.1. Machine Learning Techniques

Machine learning (ML) is typically described as a branch of “Artificial Intelligence” that is closely related to data mining, computational statistics and analytics, and data science, particularly focusing on allowing systems to learn from historical data [34]. As a result, machine learning models are often made up of a set of rules, procedures, or complex functions and equations. These features can be used to uncover intriguing data patterns, recognize sequences or anticipate behavior. As a result, ML could be useful in the field of cybersecurity. Figure 2 depicts a summarized view of the most frequently used machine learning techniques for cybersecurity. The taxonomy is primarily divided into three sections, namely deep learning models, shallow models, and reinforcement learning.

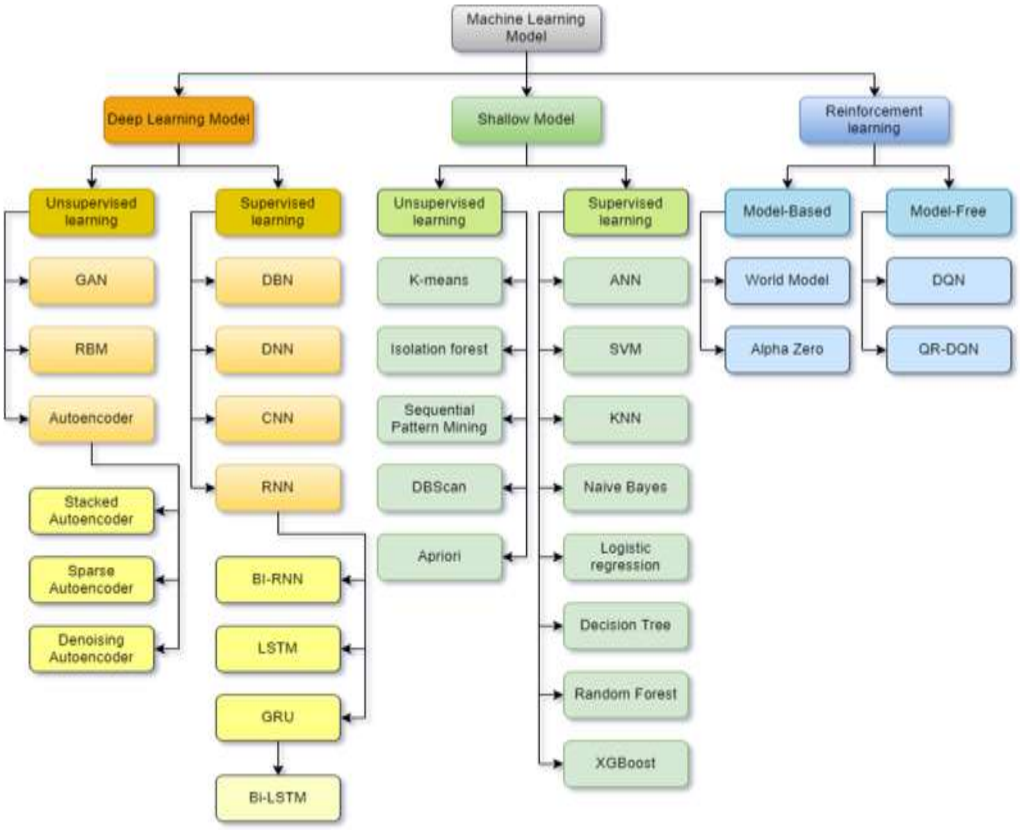

Figure 2. Taxonomy of machine learning algorithms.

Machine learning algorithms are further classified into supervised learning and unsupervised learning. In supervised learning, the models usually do not have a dependent variable and mostly rely on the internal patterns available in the dataset to group the data into different categories. This can be achieved using different algorithms, such as K-means, Sequential Pattern Mining, DB scan, and the Apriori algorithm. In supervised learning, the models usually have class labels to verify the predictions. Naïve Bayes, for example, uses probabilistic distribution to identify to which category a class label belongs. Decision trees create a tree-like structure based on a training set. For prediction, once the tree is built, any unknown record can be sorted based on the tree structure. Random forest uses a similar approach, but instead of building one decision tree, it builds multiple decision trees and then uses a voting scheme to classify a record. Because of the collective nature of the decision-making process, random forest usually has higher classification accuracy. Support vector machine (SVM) works by creating a linear decision boundary from the dataset. This can be compared to binary classification. SVMs are also capable of transforming the data using a kernel trick. This allows SVMs to classify nonlinear datasets as well.

4.2. Stages of a Attack in Network

Organizations can assess the network security risk to them and can identify certain security threats. They can then implement security controls or measures against these threats. They can utilize the National Institute of Standards and Technology (NIST) Special Publications, although they may not be a US federal agency or related contractor [35]. NIST Special Publications provide step-by-step guidance for applying a risk management framework to federal information systems. In this guidance, a set of security issues are identified and common controls or measures against these security issues/threats are listed. In a recent study, machine learning tools were suggested as efficient controls or measures. Such measures can be applied to all five phases of a Network/cyber-attack.

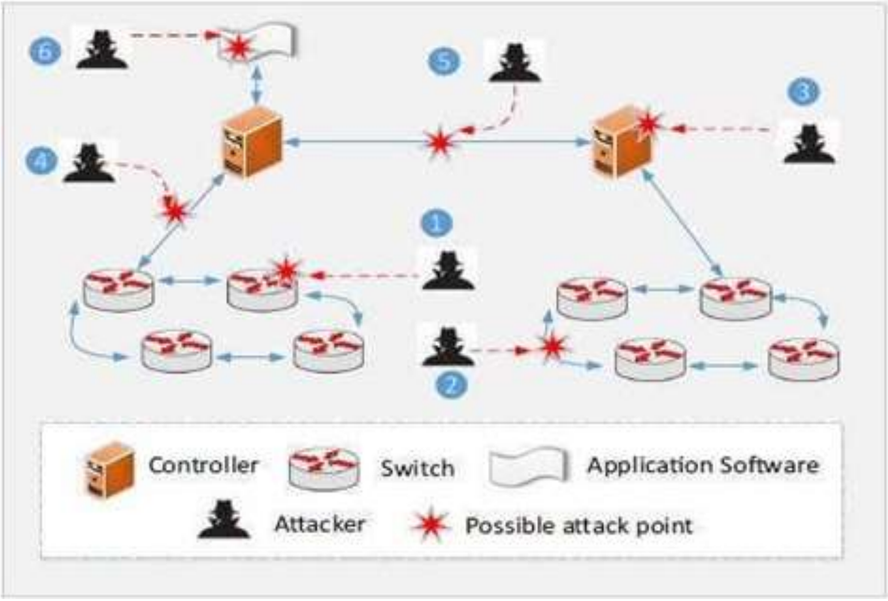

Figure 3. Possible attack points

There are five phases of a cyber-attack. They are reconnaissance, scan, attack (denial-of-service attacks, gain access using the application and operating system attacks, network attacks), maintain access (using Trojans, backdoors, rootkits, etc.), and cover tracks and hiding. An interruption at any phase can either interrupt or halt the entire process of attack. Machine learning algorithms can be used in all of these phases to help fight against cyber-attacks by disrupting the attacker's workflow.

4. Conclusion

The importance of cybersecurity and machine learning technology, we looked at how machine learning techniques are utilized to make data-driven intelligent decision-making in cybersecurity systems and services successful. The focus was on machine learning advancements and difficulties in the cybersecurity area. Deep learning is a prominent algorithm employed in several cybersecurity areas. Considering several traditional methods and machine learning methods deep learning algorithms are considered a robust way to solve problems. From this study, it is clear that most of the deep learning algorithms come up with a better accuracy rate, which will help build a real-time application for analyzing malicious activities over the network.

References

[1]. Geer, D.; Jardine, E.; Leverett, E. On market concentration and cybersecurity risk. J. Cyber Policy 2020, 5, 9–29.

[2]. Tolle, K.M.; Tansley, D.S.W.; Hey, A.J. The fourth paradigm: Data-intensive scientific discovery [point of view]. Proc. IEEE 2011,99, 1334–1337.

[3]. Alghamdi, M.I. Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. Int. J. Interact. Mob. Technol. 2020, 14, 210–224

[4]. Benioff, M. Data, data everywhere: A special report on managing information (pp. 21–55). The Economist, 27 February 2010.

[5]. Cost of Cyber Attacks vs. Cost of Cybersecurity in 2021|Sumo Logic. Available online:https://www.sumologic.com/blog/cost- of-cyber-attacks-vs-cost-of-cyber-security-in-2021/(accessed on 10 May 2022).

[6]. Anwar, S.; Mohamad Zain, J.; Zolkipli, M.F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms 2017, 10, 39.

[7]. Mohammadi, S.; Mirvaziri, H.; Ghazizadeh-Ahsaee, M.; Karimipour, H. Cyber intrusion detection by combined feature selection algorithm. J. Inf. Secur. Appl. 2019, 44, 80–88.

[8]. Tapiador, J.E.; Orfila, A.; Ribagorda, A.; Ramos, B. Key-recovery attacks on KIDS, a keyed anomaly detection system. IEEE Trans. Dependable Secur. Comput. 2013, 12, 312–325.

[9]. R. Vinayakumar, K. Soman, P. Poornachandran, Evaluating effectiveness of shallow and deep networks to intrusion detection system, in: Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on, IEEE, 2017, pp. 1282–1289.

[10]. N. Shone, T. N. Ngoc, V. D. Phai, Q. Shi, A deep learning approach to network intrusion detection, IEEE Transactions on Emerging Topics in Computational Intelligence 2 (1) (2018) 41–50.

[11]. R. Vinayakumar, K. Soman, P. Poornachandran, Applying convolutional neural network for network intrusion detection, in: Advances in Computing,

[12]. Communications and Informatics (ICACCI), 2017 International Conference on, IEEE, 2017, pp. 1222–1228.

[13]. G. Kim, H. Yi, J. Lee, Y. Paek, S. Yoon, Lstm-based systemcall language modeling and robust ensemble method for designing host-based intrusion detection systems, arXiv preprint arXiv:1611.01726.

[14]. R. C. Staudemeyer, C. W. Omlin, Evaluating performance of long short-term memory recurrent neural networks on intrusion detection data, in: Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference, ACM, 2013, pp. 218–224.

[15]. R. Vinayakumar, K. Soman, P. Poornachandran, Long shortterm memory based operation log anomaly detection, in: Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on, IEEE, 2017, pp. 236–242.

[16]. J. Saxe, K. Berlin, Deep neural network based malware detection using two dimensional binary program features, in: Malicious and Unwanted Software (MALWARE), 2015 10th International Conference on, IEEE, 2015, pp. 11–20.

[17]. G. E. Dahl, J. W. Stokes, L. Deng, D. Yu, Large-scale malware classification using random projections and neural networks, in: Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on, IEEE, 2013, pp. 3422–3426.

[18]. W. Huang, J. W. Stokes, Mtnet: a multi-task neural network for dynamic malware classification, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2016, pp. 399–418.

[19]. R. Rahul, T. Anjali, V. K. Menon, K. Soman, Deep learning for network flow analysis and malware classification, in: International Symposium on Security in Computing and Communication, Springer, 2017, pp. 226–235.

[20]. R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, A. Thomas, Malware classification with recurrent networks, in: Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on, IEEE, 2015, pp. 1916–1920.

[21]. R. Vinayakumar, K. Soman, K. S. Velan, S. Ganorkar, Evaluating shallow and deep networks for ransomware detection and classification, in: Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on, IEEE, 2017, pp. 259–265.

[22]. S. Maniath, A. Ashok, P. Poornachandran, V. Sujadevi, A. P. Sankar, S. Jan, Deep learning lstm based ransomware detection, in: Control, Automation & Power Engineering (RDCAPE), 2017 Recent Developments in, IEEE, 2017, pp. 442–446.

[23]. R. Vinayakumar, K. Soman, P. Poornachandran, Deep android malware detection and classification, in: Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on, IEEE, 2017, pp. 1677– 1683.

[24]. Z. Yuan, Y. Lu, Y. Xue, Droiddetector: android malware characterization and detection using deep learning, Tsinghua Science and Technology 21 (1) (2016) 114–123.

[25]. X. Xiao, S. Zhang, F. Mercaldo, G. Hu, A. K. Sangaiah, Android malware detection based on system call sequences and lstm, Multimedia Tools and Applications (2017) 1–21.

[26]. R. Vinayakumar, K. Soman, P. Poornachandran, S. Sachin Kumar, Detecting android malware using long short-term memory (lstm), Journal of Intelligent & Fuzzy Systems 34 (3) (2018) 1277–1288.

[27]. R. Nix, J. Zhang, Classification of android apps and malware using deep neural networks, in: Neural Networks (IJCNN), 2017 International Joint Conference on, IEEE, 2017, pp. 1871–1878.

[28]. M. Yousefi-Azar, V. Varadharajan, L. Hamey, U. Tupakula, Autoencoderbased feature learning for cyber security applications, in: Neural Networks (IJCNN), 2017 International Joint Conference on, IEEE, 2017, pp. 3854–3861.

[29]. R. Vinayakumar, K. Soman, P. Poornachandran, S. Sachin Kumar, Evaluating deep learning approaches to characterize and classify the dgas at scale, Journal of Intelligent & Fuzzy Systems 34 (3) (2018) 1265–1276.

[30]. R. Vinayakumar, P. Poornachandran, K. Soman, Scalable framework for cyber threat situational awareness based on domain name systems data analysis, in: Big Data in Engineering Applications, Springer, 2018, pp. 113–142.

[31]. F. Zeng, S. Chang, X. Wan, Classification for dga-based malicious domain names with deep learning architectures, International Journal of Intelligent Information Systems 6 (6) (2017) 67.

[32]. B. Athiwaratkun, J. W. Stokes, Malware classification with lstm and gru language models and a character-level cnn, in: Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on, IEEE, 2017, pp. 2482–2486.

[33]. D. S. Katz, J. Ruchti, E. Schulte, Using recurrent neural networks for decompilation, in: 2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER), IEEE, 2018, pp. 346–356.

[34]. Kumar, A. D., Chebrolu, K. N. R., & KP, S. (2018). A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities. arXiv preprint arXiv:1810.04144.

[35]. Vazhayil, A., Vinayakumar, R., & Soman, K. P. (2018, July). Comparative Study of the Detection of Malicious URLs Using Shallow and Deep Networks. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.