Applications of Deep learning for Cyber security Approaches Using Machine Learning

AMIT KUMAR[1], DR. RAJEEV YADAV[2]

[1]Research Scholor, Amit Kumar, Shri Krishna University, Chhatarpur, Madhya Pradesh, India.
[1]asmnidp771@gmail.com

[2]Professor, DR. RAJEEV YADAV , Shri Krishna University, Chhatarpur, Madhya Pradesh, India.

Abstract

Machine learning is of rising importance in cybersecurity. The primary objective of applying machine learning in cybersecurity is to make the process of malware detection more actionable, scalable and effective than traditional approaches, which require human intervention. The cybersecurity domain involves machine learning challenges that require efficient methodical and theoretical handling. Deep learning is an advanced model of traditional machine learning. This has the capability to extract optimal feature representation from raw input samples. This has been applied towards various use cases in cyber security such as intrusion detection, malware classification, android malware detection, spam and phishing detection and binary analysis. This paper outlines the survey of all the works related to deep learning based solutions for various cyber security use cases.

Keywords:*Cybersecurity,Machine Learning, Deep Learning, Application, Intrusion Detection, Malware Detection, Android Malware Detection*

1. INTRODUCTION

Cybersecurity refers to technologies and techniques that protect programs, networks, computers and data from being damaged, attacked or accessed by unauthorized people [1]. Cybersecurity covers various situations, from corporate to mobile computing, and can be divided into several areas. These are: (i) network security, which focuses on preventing cyber-attackers or intruders from gaining access to a computer network (ii) application security, which considers keeping devices and software free of risks or cyber-threats; (iii) information security, which primarily considers the security and privacy of relevant data; and (iv) operational security refers to the procedures for handling and safeguarding data assets. Traditional cybersecurity solutions include a firewall, antivirus software or an intrusion detection system in network and computer security systems. Data science is driving the transformation, where machine learning, an essential aspect of "Ar- tificial Intelligence", can play a vital role in discovering hidden patterns from data. Data science is pioneering a new scientific paradigm, and machine learning has substantially impacted the cybersecurity landscape [2]. With the advancement of technologies pertinent to launching cyber threats, attackers are becoming more efficient, giving rise to an increasing number of connected technologies. The graph in Figure1 depicts timestamp data in terms of a specific date, with the x-axis representing the matching popularity and the y-axis representing the corresponding popularity in the range of 0 (minimum) to 100 (maximum). It is observed that the popularity values of cybersecurity and machine learning areas were less than 30 in 2015, and they exceeded 70 in 2022, i.e., more than double in terms of increased popularity. In this study, we

focus on machine learning in cybersecurity, which is closely related to these areas in terms of security, intelligent decision making and the data processing techniques to deploy in real-world applications. Overall, this research is concerned with security data, using machine learning algorithms to estimate cyber-hazards and optimize cybersecurity processes. This project is also useful for academic and industrial researchers interested in studying and developing data-driven smart cybersecurity models using machine learning approaches.

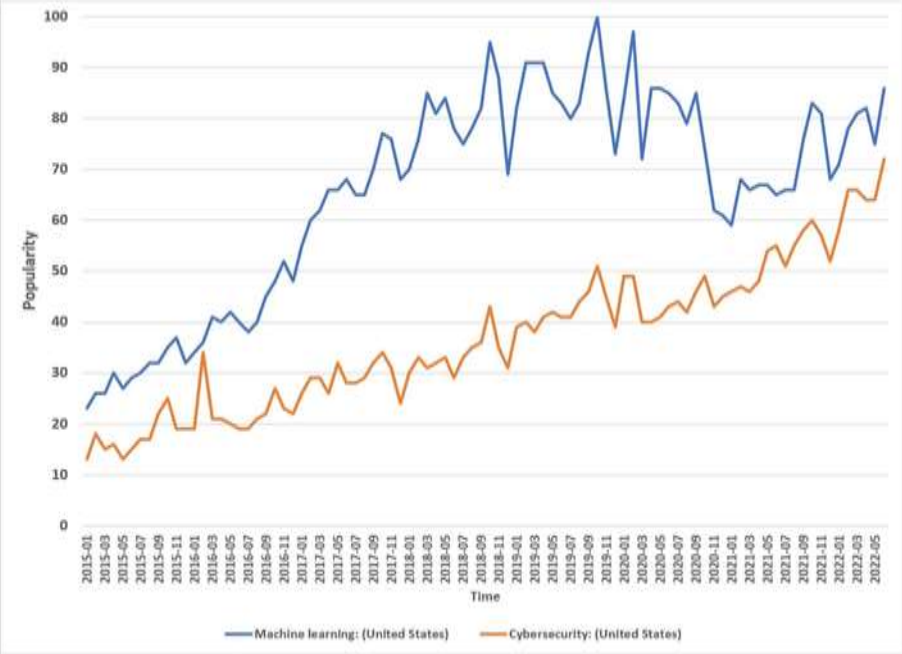

Figure 1. Google Trend for machine learning vs. data science vs. cybersecurity from 2015 to present.

Preventing cybersecurity attacks beyond a set of fundamental functional needs and knowledge about risks, threats or vulnerabilities requires analyzing cybersecurity data and building the right tools to process them successfully. Several machine learning techniques, which include but are not limited to feature reduction, regression analysis, unsupervised learning, finding associations or neural network-focused deep learning techniques, can be used to effectively extract the insights or patterns of security incidents. This is briefly discussed in the "Machine learning techniques in cybersecurity" section. These learning techniques can detect anomalies or malicious conduct and data-driven patterns of related security issues and make intelligent judgments to avert cyber-assaults.

Machine learning is a partial but significant departure from traditional well-known security solutions, including user authentication and access control, firewalls and cryptography systems, which may or may not be effective in meeting today's cyber business needs [3]. The critical difficulty is that domain experts and security analysts fix these manually in situations where ad hoc data management is required [4]. However, as a growing number of cybersecurity incidents in various formats are emerging over time, traditional solutions have proven ineffective in managing these cyber-hazards. As a result, a slew of new, complex attacks emerges and spreads rapidly over the network. Thus, several academics apply diverse

data analytic and knowledge extraction models to create cybersecurity models, which are covered in the section "Machine learning techniques in cybersecurity", based on the efficient identification of security insights and the most recent security trends that may be more relevant. According to research, addressing the cyber problem necessitates the development of more flexible and efficient security systems that can adapt to attacks and update security policies to eradicate them on a timely basis intelligently. To do this, a huge amount of relevant cybersecurity data collected from different sources, such as network and system sources, must be analyzed.

2. MACHINE LEARNING TECHNIQUES IN CYBERSECURITY

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 [5]. 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. Figure4depicts 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.

Machine learning algorithm are further classified into and 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 [5]. 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 a binary classification. SVMs are also capable of transforming the data using a kernel trick. This allows SVMs to classify nonlinear datasets as well.

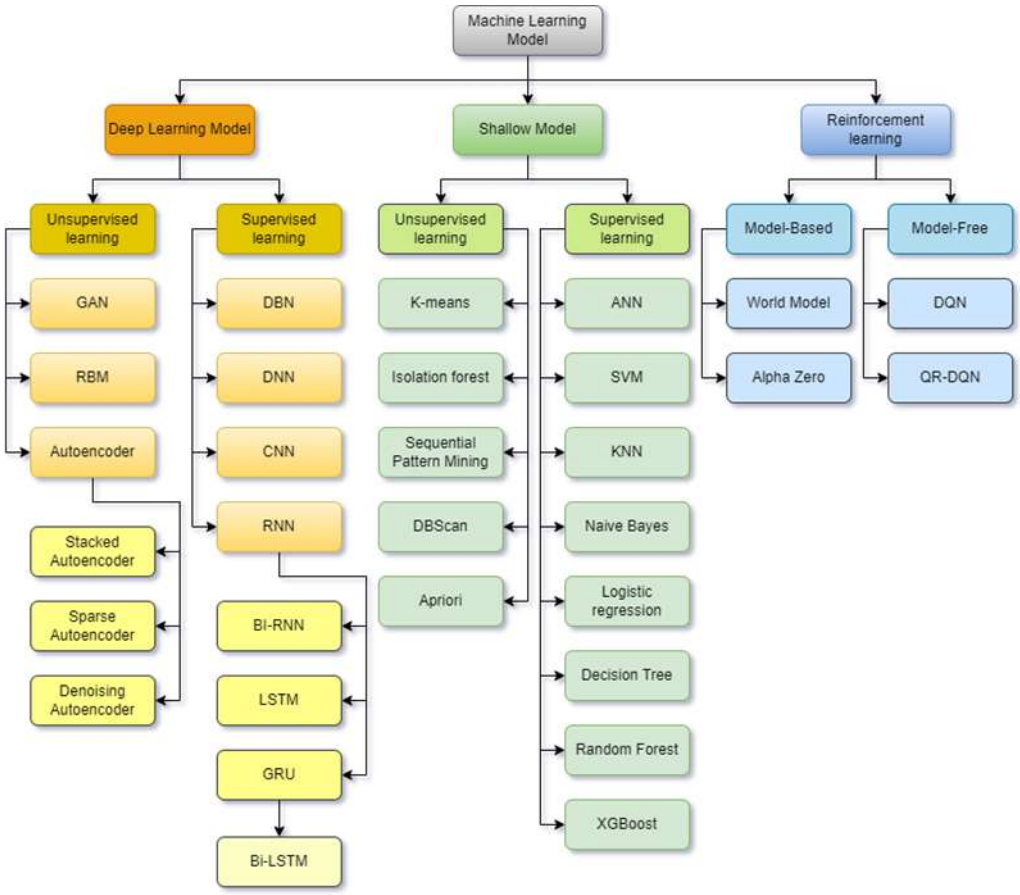

Figure 2. Taxonomy of machine learning algorithms.

2.1. Stages of a Cyber-Attack

Organizations can assess the cybersecurity 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 [6]. 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 [7]. Such measures can be applicable to all five phases of a cyber-attack.

There are five phases of a cyber-attack. They are reconnaissance, scan, attack (denial- of-service attacks, gain access using 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.

3. Cybersecurity applications

3.1. Intrusion detection

An intrusion detection system (IDS) has been developed that's capable of detection every kind of network attacks within the environments. IDS detect malicious network activities by analyzing the collected packets, alarms to 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 network is been assessed into Host based intrusion detection (HIDS) which involves in putting package and monitors 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 the 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 looks a series of bytes or sequence with malicious network and helps in track down the detail log of the system which cause false alarm. Anomaly based IDS: It helps in identifying the anomalies and indicates serious and rare events overt the system and rectifies the unusual traffic pattern in a network. To resolve the disadvantage of these two detection method Hybrid IDS has been proposed which combines the complexity of anomaly and issue detection system and gets with new framework. Now-a-days, self-learning system becomes one of the prominent methods. Machine learning is one of the powerful concepts. Most of the ML solutions resulted in achieving the high false positive rate and high machine computation. This is due to most of machine learning techniques comes with the learning patterns among small-scale, low-level feature patterns of traditional and attack connections 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 high advanced hierarchic sequence. In [9] proposed a model for novel deep learning approach in NIDS operation over networks, with combination of deep and shallow learning methods. This helps in analysis of network traffic over non symmetric deep auto encoder technique (NDAE). In [10] a brief study explains that Long short term memory(LSTM), Recurrent neural network(RNN), Convolution neural network(CNN) performs well in IDS systems when compared to other machine learning algorithms. CNN with n-gram technique is briefly discussed along with hybrid network such as CNN, CNNrecurrent neural network (CNN-RNN), CNN-long short-term memory (CNNLSTM) and CNN-gated recurrent unit (GRU).These techniques helps in identification of good and bad network ID in network connections. CNN has the capacity to gain high level feature representation from low level feature sets during 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 in capture of 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 storage of parameters in a small space. This method is considered as fast and efficient approach in sequential matrix application. Application of deep neural networks is leveraged for intrusion detection by [11]. Recently, [12] discussed the various security issues in autonomous vehicles.

3.2. Malware detection

Malwares are programs which disrupts the data, files in the system which reduces the vulnerability and performance. In some cases it will lead to total corruption of system or a server. These are easily passed through various environments using unauthorized software tools. There is existing some works in which deep learning has become one of the prominent methods in malware analysis. The binary and multiclassifier techniques are used for classification which gives better result when processed with rectified linear unit activation functions and dropout over the hidden networks. The deep learning approach applied with 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 backpropagation method helps in speeding up the learning process over the network. The echo state networks (ESNs) and recurrent neural networks (RNNs) helps in extracting full information by random temporal projection technique. Max pooling is used for non-linear sampling of data and logistic regression for final classification of data. In [13] discussed an advances malware technique known as Ransomware. It is a kind of crypto viral extortion which helps encrypt the files and gather information without other knowledge. In [14] deep learning algorithm LSTM is been applied on API calls by binary sequence classification method. The evaluated the performance of classical machine learning classifiers and deep neural networks on malware detection.

3.3. Android malware detection

Android device has becoming a popular nowadays among peoples. Malware detection becomes a big challenge in android platform. Deep learning along with NLP comes with a great breakthrough in this area [15] Droid detector is a Google app helps in 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. In [16] comes up with semantic information extraction from system call sequence method using NLP which helps in construction of deep learning model. LSTM model is constructed with effective number of hidden layers to achieve better result. Time cost function is used for classification by implementing different framework like Tensorflow to speed up the process. This model is been compared with n-gram model which is considered as superior detection method in android malware. Hyper parametric tuning is been done in LSTM network, LSTM-RNN network topology explains how the architecture helps in get better result. The effectiveness of the API call sequence is been studied, To perform this CNN is been approached by discussing the training size and sequence length which gives better indication in false and negative positive.

3.4. Domain name generation algorithms (DGAs)

Domain fluxing malwares are possessed through domain generation algorithm(DGA).These malwares encodes through domain or IP address by blocking the network from further communication to server and the host [16]. The detailed study on DNS log collection and deep learning for detecting malicious domain names in large scale is discussed in [17].The explains DNS logs in side LAN environment which use deep learning algorithms for

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 moreover these algorithms remain as robust in an adversarial environment. In [18] describes a detail study on statistical feature approach on DGA systems by splitting the features into domain length, domain level using n-gram technique. In this approach 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. Deep learning technique helps in discrimination of DGA domains from non DGA domains. In [17] focused mainly on Character based method 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 training phase along with embedding technique. To get a better predictive accuracy CMU model is implemented along with Bidirectional RNN. The NYU and Invincea models are discussed with CNN and hybrid architecture of CNN is explained along with MIT model. All this models consists of multiple layers and are termed as most extensive architectures. The LSTM network comes up with an advantage of featureless extraction of raw domain names as an input is also discussed. proposed a unique framework which correlated the data's of DNS, URL and Email to increase malicious activities detection rate.

3.5. Spam And Phishing Detection

The study shows that the 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 leaning techniques with Natural language processing (NLP). In [18] represented the phishing techniques over mail using unbalanced dataset. Mainly in this various techniques such as term frequency-inverse document frequency (TF-IDF), Nonnegative Matrix Factorization (NMF), 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. In which LR and MLB comes with high metric performance. In [19] neural network approach is discussed by applying pearl script for feature extraction which helps to get 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. In [20] discussed about the NLP feature extraction techniques using methods such as character level embedding and word embedding. A comparative study is made among Support vector machine (SVM) using character level and CNN using both character and word embedding techniques. In which CNN using word embedding gives a better result. In [21] showed a new LSTM approach in which dataset are considered as a hierarchical email architecture by considering it as sentences and words. Bidirectional LSTM is used for both cases which helps in compute the weight and estimates the phishing probability over the data during the network computation. In [22] neural network is used for classification of URL phishing it consists of three layer linear network which makes the topology very light and compact. Malicious threat over URL's is been analyzed by character

sequence. 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 URL's with faster web page response. In [23] the application of CNN is leverage for image spam detection. In [24] discussed the application of CNN and CNN-LSTM for phishing URL detection and compared with bi-gram text representation. Recently, a shared task on phishing email detection was organized as part of CODASPY'18 conference and the detailed information.

3.6. Traffic Analysis

In [25] the density and the volume of internet traffic is been increasing day by day. Identification of data flow through the network is considered as a major problem in traffic analysis. In [26] discuss traditional method using Artificial neural network and deep learning methods and result shows that in feature learning, unknown protocol identification this approach very well but it could give better adaptation in non-automation method in traditional method. Deep packet framework for extracting features automatically form network traffic using Deep learning method is proposed in these packets help in handle sophisticated task like multi challenging, traffics etc. In [28] proposed an architecture for Shallow and deep network for secure shell protocol. In [29] 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.

3.7. Binary Analysis

Binary analysis is a powerful security analysis tool which 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. Now-a-days automated analysis method is combined with deep learning method which has overcome the pattern based limitations . In [30] discussed about that different problems faced in binary analysis and how it 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 rmsprop method. This is also been discussed with background behind all networks with time function, error analysis, function identification and limitation of network. In [31] also came with 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 tokenization scheme. These helps in extraction of higher level structure from lower level binary structure. In [32] presents a new system EKLAVYA which helps in recovering function type signatures from disassembled binary codes using RNN network. Argument recovery module on RNN is implemented using techniques like saliency mapping and sanitization. This system helps in learn calling conventions and idioms with high level accuracy parameter. In [33] discussed deep learning method on assembly codes which help to analysis the software weakness. In this TextCNN is been analyzed using Instruction2vec and word2vec which has given high accuracy in classification of text data.

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 cyber security areas. Considering several traditional methods and machine learning methods deep learning algorithms considered as a robust way to solve problems. From this study it is clear that most of the deep learning algorithms comes up with better accuracy rate, which will be helpful in building an real time application for analyzing malicious activities over 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.