Deep learning based system for network cyber threat detection.

Research Scholar
Naga Venkata Aswini Pavan Kumar Inguva
University of the Cumberlands

Research Supervisor
Clint Taylor
University of the Cumberlands
.

Abstract— New organization innovations and ideal models are delivering existing interruption discovery and protection techniques outdated. Specifically, the impending fifth era (5G) versatile innovation with enormous volumes of data and high transmission rates is presenting new difficulties on network safety guard frameworks. In such manner, this paper proposes a framework for network digital dangers recognition in 5G portable organizations by utilizing profound learning strategies with factual highlights acquired from network streams. Since these highlights are payload-free, they can be registered even with encoded traffic. The framework dissects network traffic progressively and, moreover, can adjust to oversee traffic variance. This proposition has been assessed in a botnet setting, arriving at sensible arrangement exactness. Additionally, the model forecast runtime has likewise been assessed with an assortment of profound learning systems and a wide scope of traffic loads. The test results show that the model is appropriate in a genuine 5G situation. Tis paper represent the various DDOS attacks, IMP attacks, TCP\IP it attacks detection using deep learning techniques.

***Index Terms*— cyber-attacks, cyber threat, intrusion detection system, dep learning method, machine learning techniques, Jupiter anaconda navigator tool, WEKA simulation tool, KDD cup data set, performance matrix, etc.**

I INTRODUCTION

In this era of technical modernization, explosion of new opportunities and efficient potential resources for organizations have emerged but at the same time these technologies have resulted in threats to the economy. In such a scenario proper security measures plays a major role. Now days', hacking has become a common practice in organizations in order to steal data and information. This highlights the need for an efficient system to detect and prevent the fraudulent activities. Cyber security is all about the protection of systems, networks and data in the cyberspace. Malware remains one of the maximum enormous security threats on the Internet. Malware are the software's which indicate malicious activity of the file or programs. These are unwanted programs since they cause harm to the intended use of the system by making it behave in a very different manner than it is supposed to behave. Solutions with Antivirus and blacklists are used as the primary weapons of resistance against these malwares. Both approaches are not effective. This can only be used as an initial shelter in real time malware detection system. This is primarily due to the fact that both approaches are completely fails at detecting the new malware that is created using polymorphic, metamorphic, domain flux and IP flux.

Machine learning algorithms have played a pivotal role in several use cases of Cyber security [1]. Fortunately, deep learning approaches are prevailing subject in recent days due to the remarkable performance in various long-standing artificial intelligence (AI) supervised and unsupervised challenges [2]. The efficacy of deep learning architectures are transformed to various use cases of cyber This paper evaluates the effectiveness of deep neural network (DNN) for cyber security use cases: Android malware classification, incident detection and fraud detection

I DEEP LEARNING METHOD

Deep learning is an AI function that mimics the workings of the human brain in processing data for use in detecting objects, recognizing speech, translating languages, and making decisions. Deep learning AI is able to learn without human supervision, drawing from data that is both unstructured and unlabeled.

Deep learning applications are used in industries from automated driving to medical devices. Automated Driving: Automotive researchers are using deep learning to automatically detect objects such as stop signs and traffic lights. In addition, deep learning is used to detect pedestrians, which helps decrease accidents.

Various types of deep learning method is given below:

- Convolutional Neural Networks (CNNs)
- Long Short Term Memory Networks (LSTMs)
- Recurrent Neural Networks (RNNs)
- Generative Adversarial Networks (GANs)
- Radial Basis Function Networks (RBFNs)
- Multilayer Perceptrons (MLPs)
- Self-Organizing Maps (SOMs)
- Deep Belief Networks (DBNs).

Machine learning techniques:
Machine learning (ML) is a type of artificial intelligence (AI) that allows software applications to become more accurate at predicting outcomes without being explicitly programmed to do so. Machine learning algorithms use historical data as input to predict new output values.

INTRUSION DETECTION SYSTEM, IDS

With the enormous growth of computer networks and the huge increase in the number of applications that rely on it, network security is gaining increasing importance. Moreover, almost all computer systems suffer from security vulnerabilities which are both technically difficult and economically costly to be solved by the manufacturers. Therefore, the role of Intrusion Detection Systems (IDSs), as special-purpose devices to detect anomalies and attacks in a network, is becoming more important.

Traditionally, intrusion detection techniques are classified into two categories: misuse (signature-based) detection and anomaly detection. However, some researchers have recently proposed the idea of hybrid detection to reap the advantage of misuse detection by having a high detection rate on known intrusions as well as the ability of anomaly detectors in detecting brand-new attacks. Despite the inherent potential of hybrid detection, there are still two important issues that highly affect the performance of these hybrid systems. First, anomaly-based methods cannot achieve an outstanding performance without a comprehensive labeled and up-to-date training set with all different attack types, which is very costly and time-consuming to create if not impossible. Second, efficient and effective fusion of several detection technologies becomes a big challenge for building an operational hybrid intrusion detection system.

With respect to the aforementioned shortcomings, in this thesis, we introduce a network-based intrusion detection system to recognize malicious network activities and report them to the system administrator.

III RELATED WORK

this section discusses the related work for cyber security use cases: android malware classification, incident detection and fraud detection. Static and dynamic analysis is the most commonly used approaches in Android malware detection [3]. In static analysis, android permissions are collected by unpacking or disassembling the app. In dynamic analysis, the run-time execution characteristics such as system calls, network connections, power consumption, user interactions and memory utilization. Mostly, commercial systems use combination of both the static and dynamic analysis. In Android devices, static analysis is preferred due to the following advantageous such as less computational cost, low resource utilization, light-weight and less time consuming. However, dynamic analysis has the capability to detect the metamorphic and polymorphic malwares. In [4] evaluated the performance of traditional machine learning classifiers for android malware detection with using the permission, API calls and combination of both the API calls and permission as features. These 3 different feature sets were collected from the 2510 APK files. All traditional machine learning classifiers performance is good with combination of API calls and permission feature set in comparison to the API calls as well as permission. [5] proposed MalDozer that use sequences of API calls with deep learning to detect Android malware and classify them to their corresponding family. The system has performed well in both private and public data sets, Malgenome, Drebin. Recently, the privacy and security for cloud computing is briefly discussed by [6]. The discussed various 28 cloud security issues and categorized those issues into five major categories. [7] proposed machine learning based anomaly detection that acts on different layers e.g., the network, the service, or the workflow layers. [8] discussed the issues in creating the intrusion detection for the cloud infrastructure. Also, how rule based and machine learning based system can be combined as hybrid system is shown. [9] discussed the security problems in cloud and proposed incident detection system. They showed how incident detection system can perform well in comparison to the intrusion detection

IV PROPOSED PROBLEM.

Intrusion Detection is a problem of identifying unauthorized users in a computer system. It is also defined as the problem of protecting computer network systems from being compromised. The first published renowned literature on computer network security is [2] where Denning discussed various security concerns, presented a definition of Intrusion Detection and discussed different types of Intrusion Detection.

An intrusion detection system is software and/or hardware designed to detect unauthorized attempts at accessing, manipulating, and/or disabling of computer system, mainly through a network, such as the internet. One of the main challenges in the security management of large-scale high-speed networks is the detection of anomalies in network traffic.

A secure network must provide the following:

- Confidentiality: Data that are being transferred through the network should be accessible only to those that have been properly authorized.

- Integrity: Data should maintain their integrity from the moment they are transmitted to the moment they are actually received. No corruption or data loss is accepted either from random events or malicious activity.
- Availability: The network should be resilient to Denial of Service attacks.

A computer should provide confidentiality, integrity and assurance against the different types of attacks. However, due to increased load and connectivity more and more system is subjected to attack by intruders and malicious users. They attempt to exploit flaw or loop holes in the operating system as well as in the application programs. We can use the cryptographic methods to secure the system but they have their own problems as password can be easily cracked, users can lose their passwords and entire crypto-system can be broken. We need to secure the system against unauthorized access by malicious user or hacker. So we need a system which is real time i.e. we would like to detect them as soon as possible and take appropriate action. This is what an intrusion detection system does. We try to build as system which create clusters from its input data by labeling clusters as normal or anomalous data instances and finally used these cluster to classify unseen network data instances as either normal or anomalous [4]. Both training and testing was done using different subset of KDD Cup 99[9] data which is very popular and widely used intrusion attack dataset.

CYBER ATTACKS DETECTION BY MACHINE LEARNING

There are several forms of network intrusions:

• Denial-of-service Attack - This is particularly a serious form of attack that has resulted in damages worth millions of dollars over the past few years. While a significant problem, Denial-of-service attacks are usually quite simple. They typically involve an attacker disabling or rendering inaccessible a network-based information resource.

• Guessing rlogin Attack - Here the intruder tries to guess the password that protects the computer network in order to gain access to it.

• Scanning Attacks - The intruder goes about scanning different ports of the victim’s system to find some vulnerable points from where they can launch other attacks.

V RESEARCH METHODLOGY:

An *intrusion detection system* is software that automates the intrusion detection process. It can be defined as security systems that can identify attempted or ongoing attacks on a computer system or network. Developing reliable and efficient intrusion detection system that will timely and accurately detect intrusions is challenging. However, it is becoming a necessary security tool in industry. Every year, businesses lose a huge amount of revenue due to improper data manipulation caused by computer network intruders.

Ideally, intrusion detection system should have an attack detection rate (DR) of 100% along with false positive (FP) of 0%. Nevertheless, in practice this is really hard to achieve. The most important parameters involved in the performance estimation of intrusion detection system are shown in Table 1
.

Parameters	Definition
True Positive (TP) or Detection Rate (DR)	Attack occur and alarm raised
False Positive (FP)	No attack but alarm raised
True Negative (TN)	No attack and no alarm
False Negative (FN)	Attack occur but no alarm

Table 2.1. Parameters for performance estimation of intrusion detection system

Detection rate (DR) and false positive (FP) are used to estimate the performance of intrusion detection system [17], which is given as bellow:

$$DC = \frac{Total\ Detected\ Attacks}{Total\ Attacks} \times 100$$

$$FP = \frac{Total\ misclassified\ process}{Total\ Normal\ Process} \times 100$$

PROPOSED PROBLEM:

Issues with the Present Intrusion Detection System

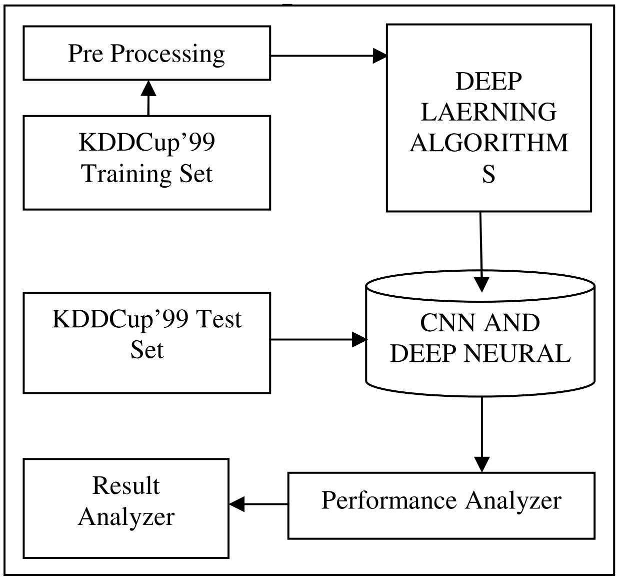
The following issues have been identified in the presently available Intrusion Detection System:

1. The following issues have been identified in the presently available Intrusion Detection System:
2. High False Alarm Rate (FAR)
3. Not completely adaptable
4. Low detection rate of u2r type of attacks
5. Low detection rate of r2l type of attacks .

Intrusion detection is the process of monitoring and analyzing the events in computer systems or networks to discover the signals of possible incidents, which attempt to compromise the confidentiality, integrity, and availability of computer resources [1]. In general, intrusion detection system use misuse based and anomaly-based detection model for detecting intrusions [4]. Misuse-based intrusion detection system are very effective for detecting known attacks but largely ineffective for detecting new attacks whose pattern has not stored in the database yet. It performs pattern matching to match an attack pattern corresponding to known attack patterns in the database. Anomaly-based intrusion detection system identifies new attacks by analyzing anomalous behavior from normal behaviors [4]. It has a relatively high detection rate for new attack, but produces many false positives [6]. It uses profiles that are developed by monitoring the characteristics of typical activities over a period of time and then compares the characteristics of current activity to thresholds related to the profile.

1. A network based intrusion detection system monitor and analyze network traffics, and use multiple sensors for detecting intrusions from internal and external networks [7]. Network intrusion detection system analyzes the information gathered by the sensors, and returns a synthesis of the input of the sensors to system administrator or intrusion prevention system. System administrator carries out the prescriptions controlled by the intrusion detection system.
2. Our network intrusion detection system approach deploys the J48 Decision tree classification algorithm [4] to learn the developed IDS with normal and anomalous traffic records applied by the training dataset. The resulting classification centric intrusion detection system is then used for fast anomaly detection in new monitoring data. The raw data and the extracted features that serve as input for the data mining algorithm. Finally, we show how the patterns can be used for classification by DEEP LEARNING classification algorithm shown in figure 4.1

6.



SIMULATION AND RESULT ANALYSIS:

Detection rate (DR) and false positive (FP) are used to estimate the performance of intrusion detection system [17], which are given as below:

$$DC = \frac{\text{Total Detected Attacks}}{\text{Total Attacks}} \times 100$$

$$FP = \frac{\text{Total misclassif ied process}}{\text{Total Normal Process}} \times 100$$

KDDCup’99 Dataset

This is the data set used for The Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99 The Fifth International Conference on Knowledge Discovery and Data Mining [9]. The competition task was to build a network intrusion detector, a predictive model capable of distinguishing between ``bad'' connections, called intrusions or attacks, and ``good'' normal connections [9]. This database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment.

In 1998, DARPA intrusion detection evaluation program, a simulated environment was set up to acquire raw TCP/IP dump data for a local-area network (LAN) by the MIT Lincoln Lab to compare the performance of various intrusion detection methods [9]. It was operated like a real environment, but being blasted with multiple intrusion attacks and received much attention in the research community of adaptive intrusion detection. In KDD99 dataset [9], each example represents attribute values of a class in the network data flow, and each class is labeled either normal or attack.

The classes in KDD99 dataset [9] can be categorized into 5 main classes (one normal class and four main intrusion classes: probe, DOS, U2R, and R2L) [4][6].

1) ***Normal*** **connections** are generated by simulated daily user behaviour such as downloading files, visiting web pages [4].

2) ***Denial of Service (DoS)*** attack [6] causes the computing power or memory of a victim machine too busy or too full to handle legitimate requests. DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users like apache2, land, mail bomb, back, etc.

3) ***Remote to Local (R2L)*** [6] is an attack that a remote user gains access of a local user/account by sending packets to a machine over a network communication, which include send-mail, and Xlock.

4) ***User to Root (U2R)*** **[6]** is an attack that an intruder begins with the access of a normal user account and then becomes a root-user by exploiting various vulnerabilities of the system. Most common exploits of U2R attacks are regular buffer-overflows, load module, Fd-format, and Ffb-config.

5) ***Probing (Probe)*** **[6] [8]** is an attack that scans a network to gather information or find known vulnerabilities. An intruder with a map of machines and services that are available on a network can use the information to look for exploits.

In 1999, the original TCP dump files were preprocessed for utilization in the Intrusion Detection System benchmark of the International Knowledge Discovery and Data Mining Tools Competition [2][9]. To do so, packet information in the TCP dump file is summarized into connections. Specifically, “a connection is a sequence of TCP packets starting and ending at some well defined times, between which data flows from a source IP address to a target IP address under some well-defined protocol” [14]. This process is completed using the Bro intrusion detection system [13], resulting in 41 features for each connection.

Features are grouped into four categories:

- *Basic Features:* Basic features can be derived from packet headers without inspecting the payload. Basic features are the first six features listed in Table 5.2[9].

- *Content Features*: Domain knowledge is used to assess the payload of the original TCP packets. This includes features such as the number of failed login attempts[9];

- *Time-based Traffic Features*: These features are designed to capture properties that mature over a 2 second temporal window. One example of such a feature would be the number of connections to the same host over the 2 second interval[9];

- *Host-based Traffic Features*: Utilize a historical window estimated over the number of connections – in this case 100 – instead of time. Host based features are therefore designed to assess attacks, which span intervals longer than 2 seconds [9].

- Detection System can usually be evaluated in terms of accuracy, detection rate and false alarm[17] as below:

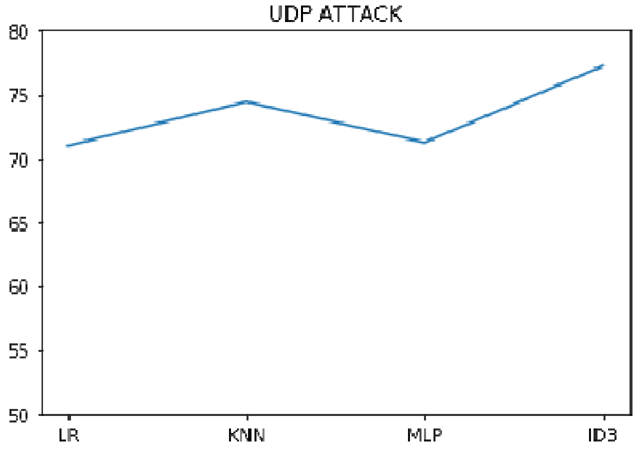
$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Detection \quad Rate = \frac{TP}{TP + FP}$$

$$False \quad Alarm = \frac{FP}{FP + TN}$$

- Where,
- FN is False Negative,
- TN is True Negative,
- TP is True Positive, and
- FP is False Positive

SIMULATE TOOL BASEDE RESULT ANLAYSIS:



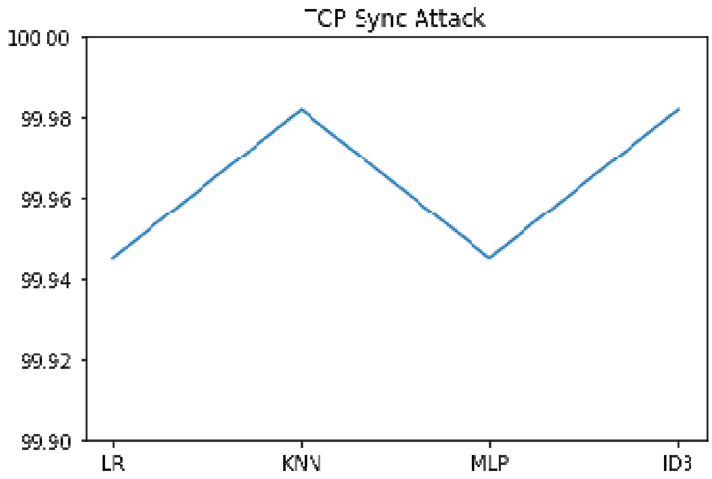


FIG 1.2 TCP\IP ATTACKS BU DEEP LEARNING METHOD.

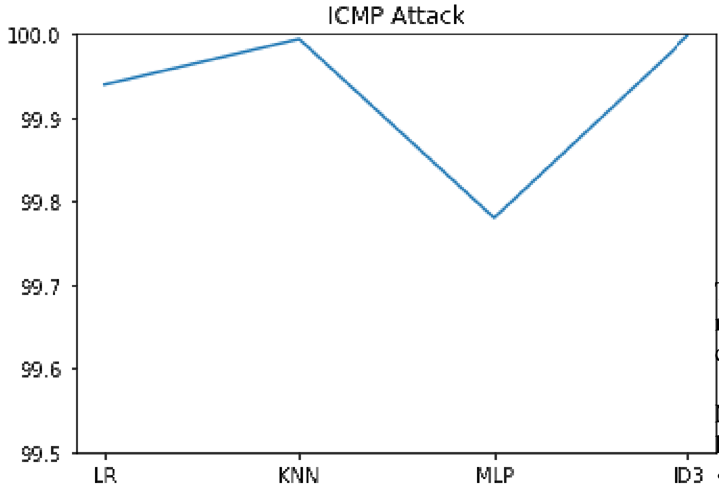
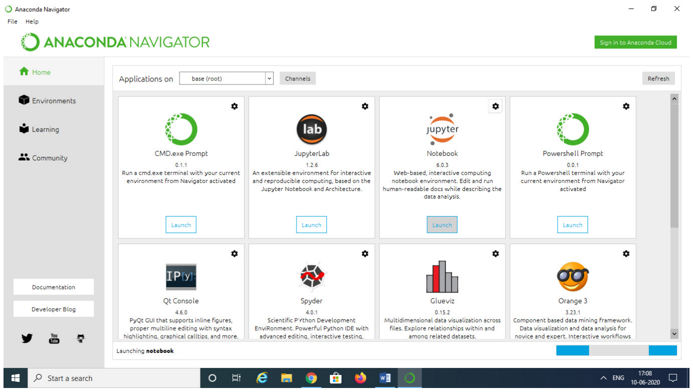


FIG 1.3 ICMP ATTACKS DETECTION BY JUPITER ANACONDA NAVIGATOR TOOL USING CNN ALGORITHMS.



Run a cmd.exe terminal with your current environment from Navigator activated

An extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture.

Web-based, interactive computing notebook environment. Edit and run human-readable docs while describing the data analysis.

Run a Powershell terminal with your current environment from Navigator activated

PyQt GUI that supports inline figures, proper multiline editing with syntax highlighting, graphical calltips, and more.

Scientific PYthon Development EnviRonment. Powerful Python IDE with advanced editing, interactive testing,

Multidimensional data visualization across files. Explore relationships within and among related datasets.

Component based data mining framework. Data visualization and data analysis for novice and expert. Interactive workflows

Launching **notebook**

FIG 1.4 JUPITER ANACONDA NAVIGATOR TOOL.

CONCLUSION AND FUTURE SCOPE:

The suggested approach called Deep learning techniques Based classification is evaluated and compared with the single machine learning classifier using KDD Cup '99 data set. The experimental results show that the CNN Based classification approach achieves better accuracy and detection rates while reducing the false alarm by detecting novel intrusions accurately. The performance of CNN AND DEEP NEURAL NETWORK has been improved by applying CNN classification. However, CNN Based classification has limitation to detect intrusions that are very similar with each other such as U2R and R2L. This paper represents the result of convolutional neural network which is the part of deep learning techniques using Jupiter anaconda navigator simulate tool for detection of various kind of cyber threat attacks detection. In this paper we have found that three types of attacks detection using deep learning techniques.

1. 1.UDP ATTACKS detection using convolutional neural network using Jupiter simulate tool.
2. ICMP tacks detection suing machine learning approach.
3. TCP/IP ATTCKS detection using deep leaning techniques along with convolutional neural network using machine learning algorithms with python language.

These kind of cyber threat detection for 5G scenario using mobile application and intrusion detection system for detection of cyber-attacks.

Many recommendations can be proposed for the future work like:

- Put and test all previous models in the real world.
- To make the previous models as general as possible, the training data set must be as variant as much as possible.

Since U2R and R2L attacks are primary attack strategies used by attackers, honey net like techniques can be considered for the future work.

REFERENCES

[1] Generations of Machine Learning in Cybersecurity, URL: https://www.cdw.com/content/dam/CDW/resources/brands/cylance/generations-ofmachine-learning-white-paper.pdf.

[2] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[3] Kapratwar, A. (2016). Static and Dynamic Analysis for Android Malware Detection.

[4] Peiravian, N., & Zhu, X. (2013, November). Machine learning for android malware detection using permission and api calls. In Tools with Artificial Intelligence (ICTAI), 2013 IEEE 25th International Conference on (pp. 300-305). IEEE.

[5] Karbab, E. B., Debbabi, M., Derhab, A., & Mouheb, D. (2017). Android Malware Detection using Deep Learning on API Method Sequences. arXiv preprint arXiv:1712.08996.

[6] Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: a survey. Computers, 3(1), 1-35.

[7] Gander, M., Felderer, M., Katt, B., Tolbaru, A., Breu, R., & Moschitti, A. (2012, August). Anomaly Detection in the Cloud: Detecting Security Incidents via Machine Learning. In EternalS@ ECAI (pp. 103-116).

[8] Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: a survey. Computers, 3(1), 1-35.

[9] Doelitzscher, F., Reich, C., Knahl, M., & Clarke, N. (2011, November). An autonomous agent based incident detection system for cloud environments. In Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on (pp. 197-204). IEEE.

[10] Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. Auditing: A Journal of Practice & Theory, 30(2), 19-50.

[11] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.

[12] Glorot, X., Bordes, A., & Bengio, Y. (2011, June). Deep sparse rectifier neural networks. In Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics (pp. 315-323).

[13] Maas, A. L., Hannun, A. Y., & Ng, A. Y. (2013, June). Rectifier nonlinearities improve neural network acoustic models. In Proc. ICML (Vol. 30, No. 1).

[14] Nair, V., & Hinton, G. E. (2010). Rectified linear units improve restricted boltzmann machines. In Proceedings of the 27th international conference on machine learning (ICML-10) (pp. 807-814).

[15] Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Kudlur, M. (2016, November). TensorFlow: A System for Large-Scale Machine Learning. In OSDI (Vol. 16, pp. 265-283).

[16] Chollet, F. (2017). Keras (2015). URL http://keras. io.

[17] Ban, T., Takahashi, T., Guo, S., Inoue, D., & Nakao, K. (2016, August). Integration of Multi-modal Features for Android Malware Detection Using Linear SVM. In Information Security (AsiaJCIS), 2016 11th Asia Joint Conference on (pp. 141-146). IEEE.

[18] Shaoning Pang, Tony Shi, Ruibin Zhang and Denis Lavrov, 2017 CDMC Task 2: Incident Detection over Unified Threat Management (UTM) operation on UniteCloud, Unitec Institute of Technology, Auckland, New Zealand, 2017.

[19] Internet Commerce Security Laboratory (ICSL), 2017 CDMC Task 3: Fraud Detection in Financial Transactions, Federation University Australia, Ballarat, VIC, Australia, 2017.

[20] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[21] Ioffe, S., & Szegedy, C. (2015, June). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In International Conference on Machine Learning (pp. 448-456).

[22] Srivastava, N., Hinton, G. E., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: a simple way to prevent neural networks from overfitting. Journal of machine learning research, 15(1), 1929-1958.

[23] Jerome H. Friedman. "Gradient Boosting Machine". In: (1999).

[24] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Vanderplas, J. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12(Oct), 2825-2830.

[25] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Detecting malicious domain names using deep learning approaches at scale. Journal of Intelligent & Fuzzy Systems, 34(3), 1355-1367.

[26] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Evaluating deep learning approaches to characterize and classify malicious URL's. Journal of Intelligent & Fuzzy Systems, 34(3), 1333-1343.

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

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

[29] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying deep learning approaches for network traffic prediction. In Advances in Computing,

Communications and Informatics (ICACCI), 2017 International Conference on (pp. 2353-2358). IEEE.

[30] Vinayakumar, R., Poornachandran, P., & Soman, K. P. (2018). Scalable Framework for Cyber Threat Situational Awareness Based on Domain Name Systems Data Analysis. In Big Data in Engineering Applications (pp. 113-142). Springer, Singapore.

[31] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 1222-1228). IEEE.

[32] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Deep encrypted text categorization. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 364-370). IEEE.

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

[34] Mohan, V. S., Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018, May). Spoof net: Syntactic patterns for identification of ominous online factors. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 258-263). IEEE.

[35] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Secure shell (ssh) traffic analysis with flow based features using shallow and deep networks. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 2026-2032). IEEE.

[36] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Evaluating shallow and deep networks for secure shell (ssh) traffic analysis. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 266-274). IEEE.

[37] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Long short-term memory based operation log anomaly detection. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 236-242). IEEE.

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

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

[40] Ra, V., HBa, B. G., Ma, A. K., KPa, S., & Poornachandran, P. DeepAntiPhishNet: Applying Deep Neural Networks for Phishing Email Detection.