A SURVEY OF CYBER SECURITY OPERATIONS BASED ON MACHINE LEARNING & DEEP LEARNING

[1]K Venkateswaralu , [2]J Avinash , [3]R Koteswaramma, [4]D Nilima Priyadharshini
[1,2,3,4]Assistant Professor
Department of Computer Science and Engineering,
Malla Reddy College of Engineering, Hyderabad

Abstract

In past decade machine learning (ML) and deep learning (DL), has generated irresistible research interest and attracted unprecedented public attention. With the increasing integration of the Internet and social life, there is change in how people learn and work, but it also exposes them to serious security threats. It is a challenging task to protect sensitive information, data, network and computers connected systems from the unauthorized cyber attacks. For this purpose, effective cyber security is required. Recent technologies such as machine learning and deep learning are integrated with cyber attacks to provide solution to this problem. The paper surveys machine learning and deep learning in cyber security also it discusses the challenges and opportunities of using ML / DL and provides suggestions for research directions.

Keywords- Cyber security, Machine learning, Deep learning, Intrusion detection.

I. INTRODUCTION

Presently system connected by internet, such as the hardware, software & data can be protected from cyber attacks by means of cyber security. Cyber security is a set of technologies and processes designed to protect computers, networks, programs and data from attacks and unauthorized access, alteration, or destruction. As threats become more sophisticated the most recent technologies such as Machine learning (ML) and deep learning (DL) are used in the cyber security community to leverage security abilities. Nowadays, cyber security is a stimulating issue in the cyber space and it has been depending on computerization of different application domains such as finances, industry, medical, and many other important areas [11]. To identify various network attacks, particularly not previously seen attacks, is a key issue to be solved urgently[1].

This paper deals with previous work in machine learning (ML) and deep learning (DL) methods for cyber security applications and some applications of each method in cyber security operations are described. The ML and DL methods covered in this paper are applicable to detect cyber security threats such as hackers and predators, spyware, phishing and network intrusion detection in ML/DL. Thus, great prominence is placed on a thorough description of the ML/DL methods, and references to seminal works for each ML and DL method are provided [1]. And discuss the challenges and opportunities of using ML / DL for cyber security.

The rest of the survey is organized as follows:

Section II tells about cyber security, Section III is composed of Machine learning, Section IV contains survey on Deep learning and Section V dedicated to similarities and differences between Machine learning & Deep learning.

II. CYBER SECURITY

Protection of networks, computer connected devices, programs, and data from malicious attacks or unauthorized access using set of technologies is known as cyber security. Cyber security can be commonly referred as information technology security. Information can be sensitive information, or other types of

data for which unauthorized access leads to disaster. In the process of synchronizing with new upcoming technologies, security trends and threat intelligence cyber security are at high risk. However, it is essential to protect information and data from cyber attacks, to maintain cyber security.

A. Challenges of cyber security

There are many challenges in the field of cyber security. One of the most challenging elements of cyber security is the changing nature of security threats. Traditionally protecting the biggest known threats and not protecting systems against less dangerous risks was approach against maintaining cyber security.

Key challenges of cyber security are:

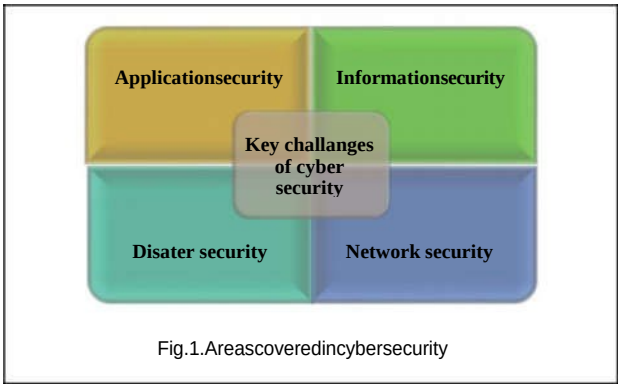

Fig.1.Areascoveredincybersecurity

• Application security: To protect applications from threats come from faults in the application design, development, deployment, upgrade or maintenance through actions that are taken during the development life-cycle is known as application security. Some basic methods used for application security are:

1. Input parameter validation.
2. User/Role Authentication &Authorization.
3. Session management, parameter manipulation & exception management.

• Information security: It protects information from unauthorized access to save privacy. Methods used are:

1. Identification, authentication & authorization of user.
2. Cryptography.

• Disaster recovery planning: It is a process that comprises performing risk assessment, generating priorities, evolving recovery strategies in case of a disaster.

• Network security: Network security includes actions that are used to protect the usability, reliability, integrity and safety of the network. Security components include:

1. Anti-virus and anti-spyware.
2. Firewall, to block unauthorized access to your network.
3. To identify fast-spreading threats, and Virtual Private Networks (VPNs) and to provide secure remote access intrusion prevention systems (IPS) is needed.

B. Types of cyber security threats

A cyber attack is a deliberate corruption of computers and servers, electronic systems, networks and data. Cyber attacks uses fake code to alter original computer code, logic or data, resulting in troublemaking consequences that lead to cybercrimes. End goal of cyber security is to prevent cyber attacks.

Following are some common types of cyber threats:

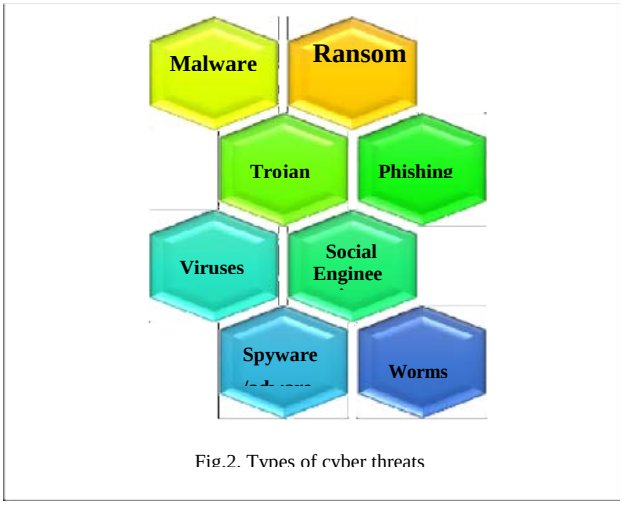

Fig.2. Types of cyber threats

• Type of activity that involves an attacker hacking system files through encryption and demanding a payment to decrypt is known as Ransomware.

• Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

• Worms are like viruses in that they are self-replicating

• An attack that relies on human interaction to trick users for breaking security to gain sensitive is Social engineering.

• A virus is a piece of malicious code that is loaded onto a machine without the user's knowledge. It spread to other computers by attaching itself to another computer file.

• Spyware/adware can be installed on computer without knowledge of user when

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-11, 2017
DOI:10.21276/ijcesr.2017.4.11.11

attachments is opened or clicked or downloaded it infects the software and collects personal information.

• Trojan virus is performing malicious activity when executed.

• Phishing is a form of fraud where phishing attacks are sent via email and ask users to click on a link and enter their personal data. However, the intention of these emails is to steal sensitive data, such as credit card or login information. There is a concerning factor about phishing that phishing emails have become sophisticated and often look just like genuine requests for information.

III. MACHINE LEARNING

Machine learning (ML) allows software applications to predict outcomes without being explicitly programmed by use of an algorithm or group of algorithms. The machine learning builds algorithms for receiving input data and uses statistical analysis to predict an output while updating outputs as new data becomes available. Prior work in cyber security based on machine learning and artificial intelligence is presented below.

Liu et al., published a systematic study on security concerns with a variety of machine learning techniques. The existing security attacks explored towards machine learning from two aspects, the training phase and the testing/inferring phase [2]. Furthermore, categorization based on current defensive techniques of machine learning into security assessment mechanisms, countermeasures in the training phase, those in the testing or inferring phase, data security and privacy is done.

Paper presented by Fraley and Dr. Cannady gives better understanding of how machine learning could be leveraged to classify various security events and alerts. They developed model to react to security events by alerting SMEs, alerting analysts or producing reports depending upon the severity of the security event. Additional support for cyber defense was discussed to further reduce the time demand for responding to critical security events[3].

Merat et al. presented different types of computer processes that can be mapped in multitasking environment for the improvement of machine learning. SHOWAN model developed by them was used to learn the cyber awareness behavior of a computer process against multiple concurrent threads [4]. The examined process starts to outperform, and tended to manage numerous tasks poorly, but it gradually learned to acquire and control tasks, in the context of anomaly detection. Finally, SHOWAN plots the abnormal activities of manually projected task and compare with loading trends of other tasks within the group.

In the article, an overview of applying machine learning to address challenges in emerging vehicular networks was presented by Ye et al. This paper introduced basics of machine learning, including major categories and representative algorithms in brief. Some preliminary examples of applying machine learning in vehicular networks to ease data-driven decision making using reinforcement learning was published [5]. Some open issues for further research also highlighted in this paper.

A systematic of the challenges associated with machine learning in the context of big data and categorization based on the V dimensions of big data was published by L'Heureux[7]. An overview of ML approaches and how these techniques overcome the various challenges were discussed in this paper. The use of the big data to categorize the challenges of machine learning enables the creation of cause-effect connections for each of the issues. Further, the creation of explicit relations between approaches and challenges enables a more thorough understanding of ML with cyber security

Golam et al., consider a data-driven next-generation wireless network model, where the MNOs employs advanced data analytics, ML and AI are used for efficient operation, control, and optimization. How ML, AI and computational intelligence play their important roles in data analytics for next-generation wireless networks are discussed in this paper. A set of network designs and optimization schemes with respect to data analytics are presented [8].

Feng and Wu presented a user-centric machine learning system which leverages big data of various security logs, alert information, and analyst insights to the identification of risky user. System provides a complete framework and solution to risky user detection for enterprise security operation center [12]. Generates

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-11, 2017
DOI:10.21276/ijcesr.2017.4.11.11

labelsfrom SOC investigation notes, to correlate IP, host, and users to generate user-centric features,

to select machine learning algorithms and evaluate performances, as well as a machine learning system in SOC production environment was briefly introduced. The whole machine learning system is implemented in production environment and fully automated from data acquisition, daily model refreshing, to real time scoring, which greatly improve and enhance enterprise risk detection and management. As to the future work, learning algorithms was proposed for further improvement of the detection accuracy. Technological trends in anomaly detection and identification and open problems and challenges in anomaly detection systems and hybrid intrusion detection systems was discussed by Patcha et al. However, the survey only covers papers published from 2002 to 2006. Unlike Modi C et al., this review covers the application of ML / DL in various areas of intrusion detection and is not limited to cloud security.[1].

Buczak et al. proposed machine-learning methods and their applications to detect intrusion [1]. Algorithms like Neural Networks, Support Vector Machine, Genetic Algorithms, Fuzzy Logics, Bayesian Networks and Decision Tree are also described in paper.

Machine-learning methods are coarsely divided into three major categories as supervised, unsupervised, and reinforcement learning. There are two phases in machine learning i.e. training and testing. In the training stage, a model is learned based on training data, whereas in the testing stage, the trained model is applied to produce the prediction.

A. Supervised Learning

Supervised learning receives a labeled data set and further divide into classification and regression types. Each training sample comes with a discrete (classification) or continuous (regression) value called a label or ground truth. The goal of supervised learning is to gain the mapping from the input feature space to the label or decision space. Classification algorithms assign a categorical label to each incoming sample. Algorithms in this category include Bayesian classifiers, k- nearest neighbors, decision trees, support vector machines, and neural networks [5]. include logistic regression, support vector regression, and the Gaussian process for regression [3].

B. Unsupervised Learning

For supervised learning, with enough data, the error rate can be reduced close to the minimum error rate bound. However, a large amount of labeled data is often hard to obtain in practice. Therefore, learning with unlabeled data, known as unsupervised learning, has attracted more attention. This method of learning aims to find efficient representation of the data samples, which might be explained by hidden structures or hidden variables, which can be represented and learned by Bayesian learning methods. Clustering is a representative problem of unsupervised learning, grouping samples into different clusters depending on their similarities. Input features could be either the absolute description of each sample or the relative similarities between samples. Classic clustering algorithms include k means, hierarchical clustering, spectrum clustering, and the Dirichlet process. Another important class of unsupervised learning is dimension reduction, which projects samples from a high-dimensional space onto a lower one without losing much information. In many scenarios, the raw data come with high dimension, and may want to reduce the input dimension for various reasons. In optimization ,clustering, and classification, the model complexity and the number of required training samples dramatically grow with the feature dimension. Another reason is that the inputs of each dimension are usually correlated, and some dimensions may be corrupted with noise and interference, which will degrade the learning performance significantly if not handled properly

[5]. Some classic dimension reduction algorithms include linear projection methods, such as principal component analysis, and nonlinear projection methods, such as manifold learning, local linear embedding, and isometric mapping[5].

C. Reinforcement Learning

Reinforcement learning deciphers how to map situations to actions, through interacting with the environment in a trial- and-error search to maximize a reward, and it comes without explicit supervision. A Markov decision process (MDP) is generally assumed in reinforcement learning, which introduces actions and (delayed)

rewards to the Markov process. The learning Q function is a classic model-free learning approach to solve the MDP problem, without the need for any information about the environment. This Q function estimates the expectation of sum reward when taking an action in a given state, and the optimal Q function is the maximum expected sum reward achievable by choosing actions. Reinforcement learning can be applied in vehicular networks to handle the temporal variation of wireless environments [5].

IV. DEEPLEARNING

Deep Learning is a sub area of Machine Learning research. It is a collection of algorithms in machine learning, used to model high-level abstractions in data. It Uses model architectures composed ofmultiplenonlinear transformations. Recently, it has made significant advances on various machine-learning tasks. Deep learning aims to understand the data representations, which can be built in supervised, unsupervised, and reinforcement learning. The input layer is at the leftmost, where each node in the figure mention of input data. The output layer is at the rightmost, corresponding to the desired outputs, whereas the layers in the middle are called hidden layers. Typically, the number of hidden layers and the number of nodes in each layer are. A deep architecture means it has multiple hidden layers in the network as shown in figure 3. However, deeper networks bring new challenges, such as needing much more training data and gradients of networks easily exploding or vanishing. With the help of faster computation resources, new training methods (new activation functions, prêt raining), and new structures (batch norm, residual networks), training such deep architecture becomes possible. Deep learning has been widely used in such areas as computer vision, speech recognition, and natural language processing and greatly improved state-of-the-art performance in these areas. Depending on applications, different structures can be added to the deep networks, e.g. convolution networks share weights among spatial dimensions, whereas recurrent neural networks (RNNs) and long short-term memory (LSTM) share weights among the temporal dimensions[5].

Deep learning aims to learn a hierarchy of features from input data. It can automatically learn features at multiple levels, which makes the system be able to learn complex mapping function directly from data. The most characterizing feature of deep learning is that models have deep architectures. Deep architecture has multiple hidden layers in the network. In contrast a shallow architecture has only a few hidden layers (1 to 2 layers). Deep learning algorithms have been extensively studied in recent years. Algorithms are grouped into two categories based on their architectures:

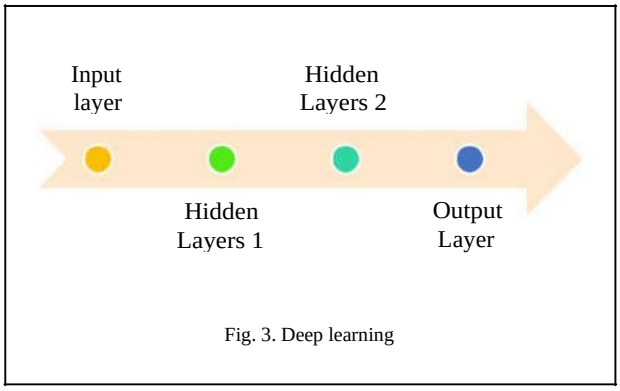

Fig. 3. Deep learning

A. Convolution neural net works(CNN)

Convolution neural networks (CNNs) has gain astonishing recognition in the field of computer vision. It has been continuously advancing the image classification accuracy. Also plays an important role for generic feature extraction such as scene classification, object detection, semantic segmentation, image retrieval, and image caption. Convolution neural network (CNNs) is most important aspect of deep neural networks in image processing. It is highly effective and commonly used in computer vision applications. The convolution neural network composed of three types of layers: convolution layers, sub sampling layers, and full connection layers.

B. Restricted Boltzmann Machines(RBMs)-

RBM is an energy-based probabilistic generative model. It is composed of one layer of visible units and one layer of hidden units. The visible units represent the input vector of a data sample and the hidden units represent features that are abstracted from the visible units. Each visible unit is connected to hidden unit, whereas no connection exists within the visible layer or hidden layer. During past years, the quality of image classification and object detection has been dramatically improved due to the deep learning method.

C. Recurrentneural Network

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-11, 2017
DOI:10.21276/ijcesr.2017.4.11.11

RNNs are used to make use of sequential information. In a traditional neural network all inputs (and outputs) are independent of each other. To predict the next word in a sentence, need to know which words came before it. RNNs are called recurrent as they perform the same task for every element of a sequence, with the output being depended on the previous computations. RNNs can make use of information in arbitrarily long sequences, but in practice they are limited to only a few steps. An online unsupervised deep learning system is used to filter system log data for analyst. In which variants of Deep Neural Networks (DNNs) and Recurrent Neural Networks (RNNs) are trained to recognize activity of each user on a network and concurrently assess whether user behavior is normal or anomalous, all in real time [10]. Developed model faced several key difficulties in applying machine learning to the cyber security domain. Model was trained continuously in an online fashion, but detection of malicious events was challenging task.

Comparative study was presented by Gavai et al. (2015) of a supervised approach and an unsupervised approach using the isolation forest method for detecting insider threat from network logs. Ryan et al. (1998) applied neural network-based approaches to train network with one hidden layer to predict the probabilities-based network intrusion [10]. A network intrusion was detected for the probability less than

But input features were not structured and did not train the network in an online fashion.

Modeling normal user activity on a network using RNNs was performed by Debar et al. (1992). The RNN was trained on a representative sequence of Unix command line arguments (from login to logout). Network intrusion detected when the trained network poorly predicts the login to logout sequence. While this work partially addresses online training, it does not continuously train the network to consider changing user habits overtime.

Recurrent neural networks have been successfully applied to anomaly detection in various alternative domains such as signals from mechanical sensors for machinery such as engines, and vehicles [10].

An inclusive analysis of text Captchas, to evaluate security, a simple, effective and fast attack on text Captchas proposed by Tang et al. Using deep learning techniques, which successfully can attack all Roman character-based text Captchas deployed by the top 50 most popular websites in the world and achieved state-of-the-art results. Success rates range from 10.1% to 90.0% [9]. A novel image-based Captcha named SA Captcha using neural style transfer techniques also presented. This is a positive attempt to security of Captchas by utilizing deep learning techniques. In this paper, deep learning techniques play two roles: as a character recognition engine to recognize individual characters and as a powerful means to enhance the security of the image-based Captcha This proved that deep learning is a double-edged sword. It can be either used to attack Captchas or improve the security of Captchas [9]. In future, they predicted existing text Captchas are no longer secure. Other Captcha alternatives are robust, and the designs of new Captchas can be simultaneously secure and usable are still challenging difficulties to be work on[9].

A new approach for detection of network intrusion using unsupervised deep learning with iterative K-means clustering proposed by Alom and Taha. In addition, unsupervised ELM, and only K-means clustering approaches were tested. From empirical evaluation on KDD-Cup 99 benchmark, it is observed that the deep learning approach of RBM and AE with k-means clustering show around 92.12% and 91.86% accuracy for network intrusion detection respectively. RBM with K-means clustering provides around 4.4% and 2.95% better detection accuracy compare to K-means and USELM techniques respectively [11].

Nichols and Robinson present an online unsupervised deep learning approach to detect anomalous network activity from system logs in real time. Models decompose anomaly scores into the contributions of individual user behavior features for increased interpretability to aid analysts reviewing potential cases of insider threat. Using the CERT Insider Threat Dataset v6.2 and threat detection recall, their novel deep and recurrent neural network models outperform Principal Component Analysis, Support Vector Machine and Isolation[10].

V. SIMILARITIES AND DIFFERENCES BETWEEN MACHINE LEARNING & DEEPLEARNING

There are many puzzles about the relationship among ML, DL, and artificial intelligence (AI). Machine-learning is a branch of AI and is closely related to computational statistics, which also focuses on prediction making using computers [1]. whereas DL is a sub-field in machine-learning research. Its motivation lies in the establishment of a neural network that simulates the human brain for analytical learning. It mimics the human brain mechanism to interpret data such as images, sounds and texts[14].

A. Similarities

• Steps involved in ML and DL

ML and DL method primarily uses similar four steps in except feature extraction in DL is automated rather than manual [12].

• Methods used in ML and DL

ML/DL are similar in these three approaches: supervised, unsupervised and semi-supervised. In supervised learning, each instance consists of an input sample and a label. The supervised learning algorithm analyzes the training data and uses the results of the analysis to map new instances. Unsupervised learning that deduces the description of hidden structures from unlabeled data. Because the sample is unlabeled, the accuracy of the algorithm's output cannot be evaluated, and only the key features of the data can be summarized and explained. Semi-supervised learning is a means of combining supervised learning within supervised learning. Semi-supervised learning uses unlabeled data when using labeled data for pattern recognition. Using semi- supervised learning can reduce

label efforts while achieving high accuracy [1].

B. Differences

ML and DL methods different in following ways:

• Data dependencies.

The main difference between deep learning and machine learning is its performance as the amount of data increases. Deep learning algorithms do not perform well when the data volumes are small, because deep learning algorithms require a large amount of data to understand the data perfectly. Conversely, machine-learning algorithm uses the established rules, thus performance is better.

• Hardware dependencies

The DL algorithm requires many matrix operations. The GPU is largely used to optimize matrix operations efficiently. Therefore, the GPU is the hardware necessary for the DL to work properly. DL relies more on high-performance machines with GPUs than machine-learning algorithms.

• Feature processing

The process of putting domain knowledge into a feature extractor to reduce the complexity of the data and generate patterns that make learning algorithms work better is known as feature processing. In ML, most of the characteristics of an application must be determined by an expert and then encoded as a data type. The performance of most ML algorithms depends upon the accuracy of the features extracted. Trying to obtain high-level features directly from data is a major difference between DL and traditional machine-learning algorithms. Thus, DL reduces the effort of designing a feature extractor for each problem.

• Problem-solving method

In Problem-solving method on applying traditional machine- learning algorithms to solve problems, traditional machine learning usually breaks down the problem into multiple sub-problems and solves the sub-problems, ultimately obtaining the result. Unlike deep learning which solves end-to-end problem.

• Execution time.

DL algorithm takes long time to train because there are many parameters in the DL algorithm. Whereas ML training takes relatively less time, only seconds to hours. The test time is exactly opposite for ML and DL. Deep learning algorithms require very little time to run during testing phase compared to ML algorithms. This is not applicable to all ML algorithms, some required short test times[1]

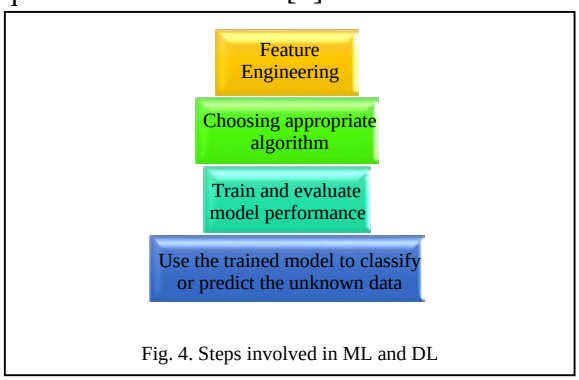

Fig. 4. Steps involved in ML and DL

V. CONCLUSION

This paper provides researchers with a strong foundation for making easier and better informed choices about machine learning and deep learning for cyber security. It was reviewed that machine learning has some challenges in handling Big Data whereas deep learning performance is better in context of big data. To improve the security, an innovative image-based captcha named SA Captcha using deep learning techniques can be used. Unsupervised deep learning of RBM and AE with iterative k-means clustering show around 92.12% and 91.86% accuracy for network intrusion detection. In future, system of network intrusion detection for cyber security with online learning approach can be deployed. Machine learning is used to develop a model which detect and highlight advanced malware, by alerting SMEs, alerting analysts or producing reports depending upon the severity of the security event. The model performs these functions with very high accuracy (90%). To detect abnormal network activity from system logs in real time, an online unsupervised deep learning approach can be used that producesinterpretable assessments of insider threat in streaming system user logs. This work has therefore accomplished its objective by providing with potential directions for future work and will hopefully serve as groundwork for great improvements of machine learning and deep learning methods for cyber security operations.

REFERENCES

[1] Yang Xin Et Al., "Machine Learning And Deep Learning Methods For Cyber security" In IEEE Journals & Magazine, May2018.

[2] Qiang Liu Et Al., "A Survey On Security Threats And Defensive Techniques Of Machine Learning: A Data Driven View", In IEEE Journals & Magazine, Vol 6, February2018.

[3] James B. Fraley And Dr. James Cannady, "The Promise Of Machine Learning In Cyber security", In Southeast conference , May2017.

[4] Soorena Merat, P.Eng, Dr. Wahab Almuhtadi, P.Eng., "Artificial Intelligence Application For Improving Cyber-Security Acquirement" In 28th IEEE Canadian Conference On Electrical And Computer Engineering, Halifax, Canada, May2015.

[5] Hao Ye, Le Liang et al., "Machine Learning for Vehicular Networks" In IEEE Vehicular Technology Magazine, April2018.

[6] Ge Wang, Jong Chu Ye et al., "Image Reconstruction Is A New Frontier Of Machine Learning", In IEEE Transactions On Medical Imaging ,Vol. 37, pp 1289 – 1296, June2018.

[7] Alexandra L'heureux et al., "Machine Learning With Big Data: Challenges And Approaches", In IEEE Journal & Magazine ,Vol 5, pp 7776 – 7797, April2017.

[8] Mirza Golam Kibria Et Al., "Big Data Analytics, Machine Learning And Artificial Intelligence In Next-Generation Wireless Networks", In IEEE Journal & Magazine, May 2018, pp2169-3536.

[9] Mengyun Tang Et Al., "Research On Deep Learning Techniques In Breaking Text-Based Captchas And Designing Image-Based Captcha", In IEEE Transactions On Information Forensics And Security,Vol13, Issue: 10,pp 2522 – 2537,Oct.2018.

[10] Aaron Tuor ,Samuel Kaplan And Brian Hutchinson, "Deep Learning For Unsupervised Insider Threat Detection In Structured Cyber security Data Streams", In Proceedings Of Ai For Cyber Security Workshop At AAAI ,Dec2017.

[11] Md Zahangir Alom And Tarek M. Taha, "Network Intrusion Detection For Cyber Security Using Unsupervised Deep Learning Approaches", In IEEE National Aerospace And Electronics Conference (NAECON), Dayton, Oh, USA, June2017.

[12] Charles Feng*, Shunning Wu And Ningwei Liu, "A User-Centric Machine Learning Framework For Cyber Security Operations Center",

In IEEE International Conference On Intelligence And Security Informatics (ISI), Beijing, China, July 2017.

[13] Ozlem Yavanoglu And Murat Aydos, "A Datasets For Machine Learning Algorithms", In IEEE International

Conference On Big Data ,Jan 2018.

[14] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "EvaluatingComputerIntrusionDetectionSystems:ASurveyofCommon Practices,"AcmComput.Surv.,vol.48,no.1,pp.1–41,2015.

[15] C. N. Modi and K. Acha, "Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review," J.Supercomput., vol. 73, no. 3, pp. 1–43, 2016.

[16] E. Viegas, A. O. Santin, A. França, R. Jasinski, V. A. Pedroni, andL.

S. Oliveira, "Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems," IEEETrans.Comput., vol. 66, no. 1, pp. 163–177, 2017.