IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Intelligent Intrusion Detection System Using Deep Learning and Extreme Machine Learning Algorithms

Mrs. T. Madhavi Kumari, Aziz Ullah Karimy

Associate Professor of Electronics and Communication Engineering, M Tech Student
College of Engineering Hyderabad,
Jawaharlal Nehru Technological University, Hyderabad, Indian

Abstract: In today's world, networks are significant, and cyber security has emerged as an essential study field. An intrusion detection system (IDS), a significant cyber security method, keeps track of the condition of the network's software and hardware. Existing IDSs still confront hurdles in increasing detection accuracy, lowering false alarm rates, and identifying novel assaults, despite decades of research. Many academics have concentrated on building IDSs that employ machine learning approaches to overcome the difficulties mentioned above. In this paper we are evaluating the performance of various classical algorithms such as SVM, Random Forest and Naive Bayes to detect attacks on network using IDS datasets such KDD, NSL but this classical algorithms unable to predict dynamic (if attacker introduce new attacks with changes in attack parameter) attacks and need to be trained in advance to detect such attacks to overcome from this problem we are evaluating performance of Deep Neural Network (DNN) algorithm with dynamic attack signatures and detection accuracy of DNN shown to be better compare to all classical algorithms. Deep learning is a field of artificial intelligence that has an impressive results and is now a hotspot for study. This survey presents an IDS taxonomy that classifies and summarizes machine learning- and deep learning-based IDS literature using data objects as the primary dimension.

Keywords: machine learning; deep learning; Extreme Machine Learning; intrusion detection system; cyber security.

1. INTRODUCTION

Because networks are having a growing impact on modern life, cyber security is an essential subject of study. The most prevalent cyber security technologies include anti-virus software, firewalls, and intrusion detection systems (IDSs). These methods defend networks against both internal and external threats. An IDS, for example, is a sort of detection system that monitors the states of software and hardware running on a network and helps to defend cyber security. In 1980, the first intrusion detection system [1] was suggested. Many competent IDS products have emerged since then. However, many IDSs still have a high false alarm rate, generating several warnings for low-threat circumstances, increasing the strain on security analysts and perhaps causing severe attacks to go unnoticed. As a result, several academics have concentrated their efforts on building IDSs that have better detection rates and lower false alarm rates. Another issue with current IDSs is that they are incapable of detecting unknown assaults. Because network environments change rapidly, new attack types and assaults occur on a regular basis. As a result, IDSs that can identify unknown threats must be developed. To solve the aforementioned issues, experts have begun to concentrate on developing IDSs utilizing machine learning techniques. Machine learning is an artificial intelligence technology that can automatically extract usable data from large datasets [2]. When enough training data is available, machine learning-based IDSs may reach excellent detection levels, and machine learning models have sufficient generalizability to detect attack variations and novel assaults. Furthermore, because machine learning-based IDSs do not rely extensively on domain expertise, they are simple to design and build. Deep learning is a type of machine learning that can generate exceptional results. Compared with traditional machine learning techniques, deep learning methods are better at dealing with big data [3]. Moreover, deep learning methods can automatically learn feature representations from raw data and then output results; they operate in an end-to-end fashion and are practical. The deep structure, which has numerous hidden layers, is one distinguishing feature of deep learning. Traditional machine learning models like the support vector machine (SVM) and k-nearest neighbour (KNN), on the other hand, have no or just one hidden layer. As a result, classic machine learning models are referred to as shallow models. These issues are the driving force behind this research, which aims to assess the performance of several traditional machine learning classifiers and deep neural networks (DNNs) when applied to NIDS and HIDS. This work assumes the following;

- An attacker aims at pretense as normal user to remain hidden from the IDS. However, the patterns of intrusive behaviors differ in some aspect. This is due to the specific objective of an attacker for example getting an un authorized access to computer and network resources.
- The usage pattern of network resources can be captured, however the existing methods ends up in high false positive rate.
- The patterns of intrusions exist in normal traffic with a very low profile over long time interval.

2. LITERATURE REVIEWS

A detailed investigation and analysis of using machine learning techniques for intrusion detection [3]. In today's cyber environment, intrusion detection is one of the most pressing security issues. A substantial number of strategies machine learning based methodologies have been invented. They are, however, not very good at detecting all forms of intrusions [4].

Machine Learning Based Botnet Identification Traffic [5].The growing sophistication of toolkits and techniques for conducting computer attacks and intrusions that are convenient to use and freely available to download, such as the Zeus botnet toolkit, has stemmed from the Internet's continuing growth. Several cyber-attacks, like spam, distributed denial-of-service (DDoS), identity theft, and phishing, are carried out through botnets.

Adaboost-based algorithm for network intrusion detection [6]. The goal of network intrusion detection is to distinguish between Internet attacks and typical Internet usage. It is a critical component of any information security system. Because of the wide range of network activities and the quick evolution of attack styles, quick machine-learning-based intrusion detection algorithms with improved detection rates and low false-alarm rates are required. The approach employs decision stumps as poor predictors. Decision stumps are used as weak predictors in this method. Both categorical and continuous characteristics are handled by the decision rules [7].

In computer networks, ensemble learning for intrusion detection [8]. The security of computer networks is crucial in today's computer systems. A variety of software technologies are now being developed in order to impose high levels of threat prevention. Intrusion Detection Systems are designed to identify intruders who have gotten beyond the "first line" of defence. A pattern recognition technique to network intrusion detection is suggested in this research [9], which is based on ensemble learning paradigms. The potentialities of such an approach for data fusion and some open issues are outlined.

3. METHODOLOGY

Today’s ICT system is considerably more complex, connected and involved in generating extremely large volume of data, big data is a term used to describe a large amount of information. This is mostly due to technological advancements and the quick deployment of a huge number of apps. Big data is a catchphrase that refers to methods for extracting useful information from massive amounts of data. It is critical to allow access to big data technologies in the realm of cyber security, notably IDS. The evolution of big data technology allows for the timely extraction of diverse patterns of legal and malicious actions from massive volumes of network and system activity data, which helps to improve IDS performance. The processing of massive data with traditional methods, on the other hand, is frequently problematic. The goal of this part is to detail the proposed framework's computational architecture and sophisticated methodologies, such as text representation methods, deep neural networks (DNNs), and DNN training processes.

A. SCALABLE COMPUTING ARCHITECTURE

The proposed scalable architecture employs distributed and parallel machine learning algorithms with various optimization techniques that makes it capable of handling very high volume of network and host-level events [10]. The scalable design additionally takes use of the general purpose graphics processing unit (GPGPU) cores' processing power for quicker and parallel network and host-level event analysis. There are two kinds of analytic engines in the framework: real-time and non-real-time. The purpose of analytic engine is to monitor network and host-level events to generate an alert for an attack By adding more computer resources, the established framework may be scaled up to analyse increasingly bigger amounts of network event data. The created framework stands out from other systems of its sort due to its scalability and real-time identification of dangerous activity using early warning signals.

B. TEXT REPRESENTATION METHODS

System calls are critical in any operating system that depicts computer activities, and they make up a massive quantity of unstructured and fragmented data that a standard HIDS utilises to identify intrusions and cyber-attacks.

We look at text representation approaches in this study to categorise process behaviours using system call trace [11]. Feature extraction, feature engineering, and feature representation methods are used in traditional machine learning methodologies. The use of sophisticated machine learning embedded approaches such as deep learning, on the other hand, can totally eliminate the need for feature engineering and feature extraction. We adopt such advanced deep learning along with text representation methods to capture the contextual and sequence related information from system calls. In this work, the system calls are converted into feature vectors using the following feature representation approaches from the field of NLP.

C. DEEP NEURAL NETWORK (DNN)

We employ an artificial neural network (ANN) approach as the computational model since it is influenced by the characteristics of biological neural networks to incorporate intelligence in our proposed method. A feed forward neural network (FFN) is a type of artificial neural network (ANN) that uses edges to transmit information from one node to the next without generating a loop. We adopt a multilayer perceptron (MLP) model which is a type of FFN having three or more layers with one input layer [12], one or more hidden layers and an output layer in which each layer has many neurons or units in mathematical notation. We use a hyper parameter selection approach to determine the number of hidden layers. Information is transferred in a forward manner from one layer to the next, with neurons in each layer being completely linked.

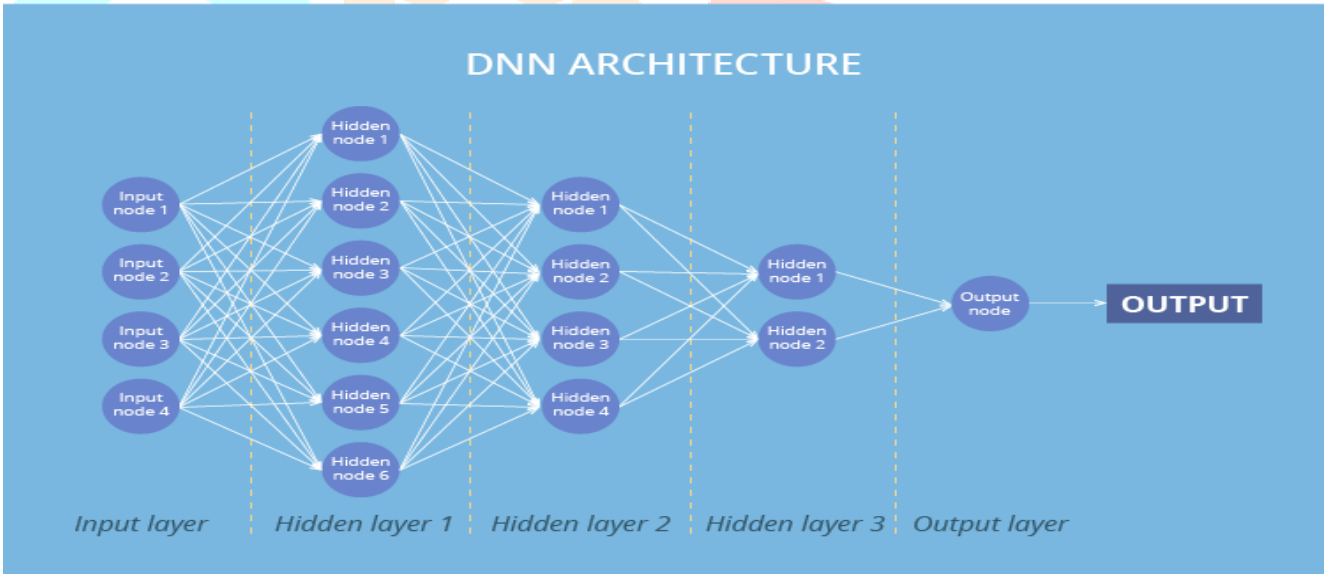

Fig 1: Architecture of DNN

D. EXTREME LEARNING MACHINE

Extreme learning machines are feed forward neural systems for grouping, relapse, bunching, inadequate estimation, pressure and highlight learning with a solitary layer or various layers of shrouded hubs, where the parameters of concealed hubs (not simply the loads interfacing contributions to concealed hubs) need not be tuned. These concealed hubs can be haphazardly doled out and never refreshed (for example they are irregular projection however with nonlinear changes), or can be acquired from their predecessors without being changed. Much of the time, the yield loads of concealed hubs are typically learned in a solitary advance, which basically sums to learning a straight model. The name "Extreme learning machine" (ELM) was given to such models by its principle designer Guang-Bin Huang. As indicated by their makers, these models can deliver great speculation execution and learn a huge number of times quicker than systems prepared utilizing back propagation.

4. RESULTS AND DISCUSSION

Extreme Learning Machine algorithm which is an advance version neural networks. This algorithm can achieve good accuracy with less execution time.

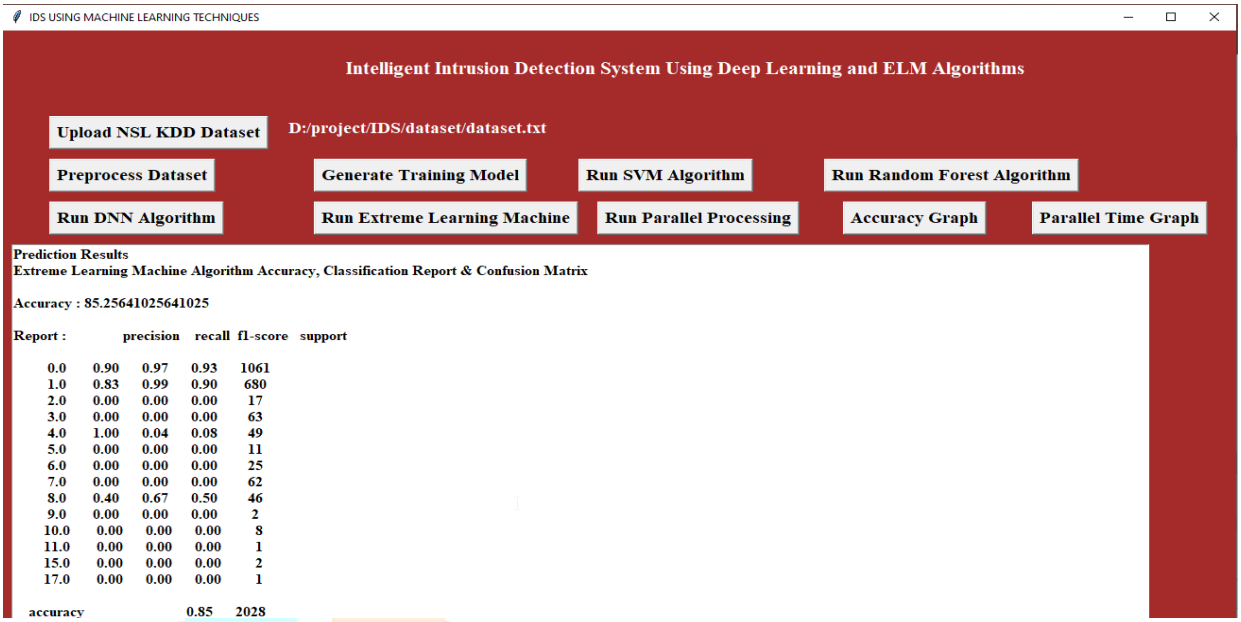

Fig 2: Extreme Learning Machine performance

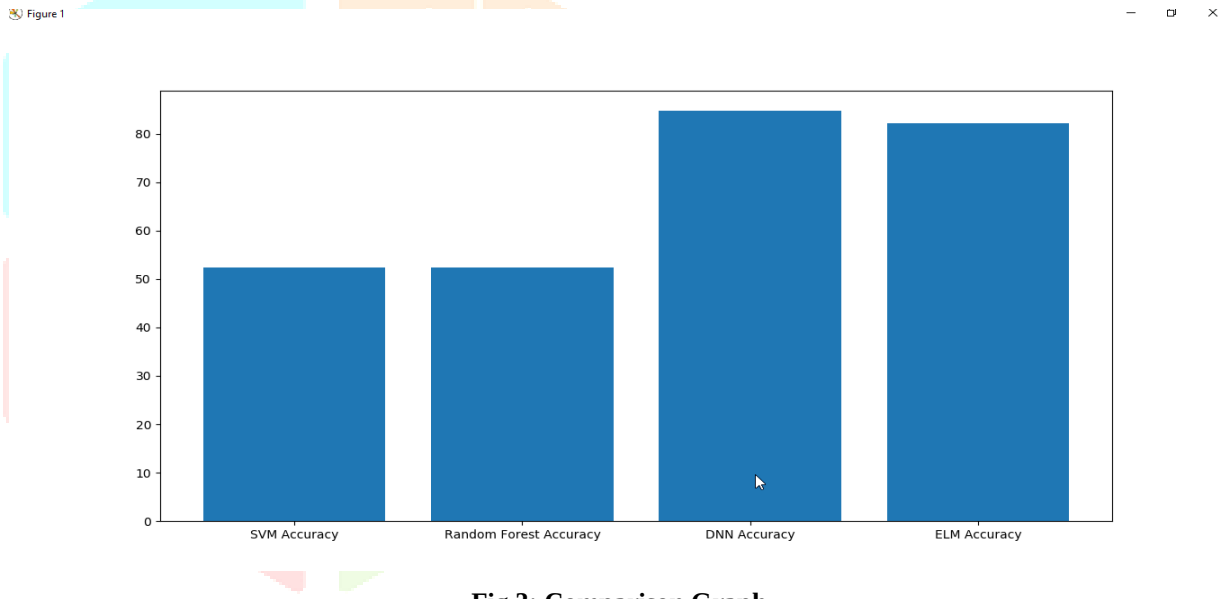

Fig 3: Comparison Graph

Above is the comparison graph between Support Vector Machine (SVM), Random Forest, Deep Neural Network (DNN) and Extreme Learning Machine (ELM).

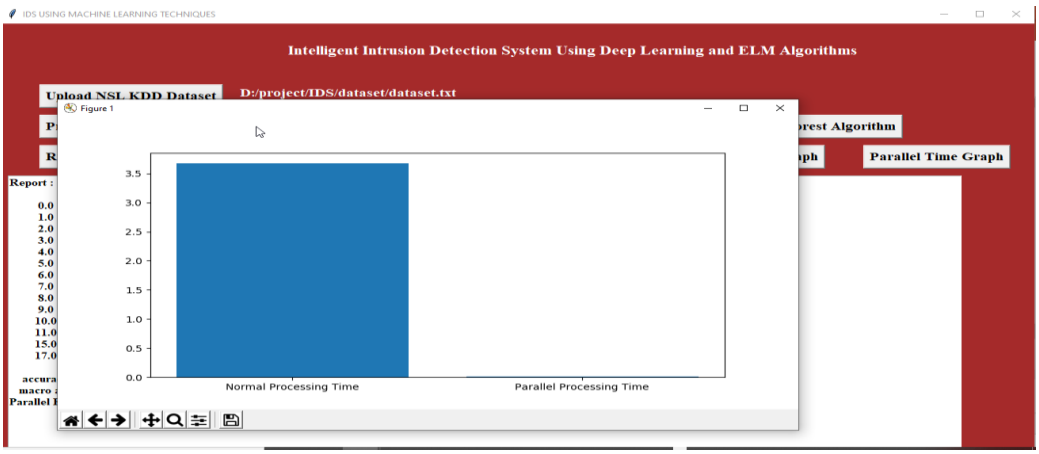

Fig 4: Comparison of Normal and parallel Processing

The above graph represents the normal and parallel processing time for IDS, which indicates that execution time with parallel processing can minimized.

5. CONCLUSION

Deep learning models are playing an increasingly important role and have become an outstanding direction of study. Deep learning approaches include multiple deep networks which can be used to improve the performance of IDSs. Compared with shallow machine learning models, deep learning models own stronger fitting and generalization abilities. In addition, deep learning approaches are independent of feature engineering and domain knowledge, which takes an outstanding advantage over shallow machine learning models. Deep learning models, on the other hand, frequently take too long to run to fulfil the real-time requirements of IDSs. Compared to DNN the Extreme machine learning algorithm will give better accuracy with less running time.

6. REFERENCES

[1] Anderson, J.P. Computer Security Threat Monitoring and Surveillance; Technical Report; James P. Anderson Company: Philadelphia, PA , USA, 1980.

[2] Preeti Mishra;Vijay Varadharajan; Uday Tupakula; A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection, IEEE Communications Surveys & Tutorials, June 2019.

[3] Said A. Salloum1, Muhammad Alshurideh, Ashraf Elnagar and Khaled Shaalan, Machine Learning and Deep Learning Techniques for Cybersecurity, Research Institute of Sciences and Engineering,University of Sharjah, Sharjah, UAE, 2020

[4] Vaibhav Nivargi, Mayukh Bhaowal, Teddy Lee, Machine Learning Based Botnet Detection, IEEE,2017

[5] Weiming Hu; Wei Hu; Steve Maybank, AdaBoost-Based Algorithm for Network Intrusion Detection, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), March 2008

[6] Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. 2015, 18, 1153–1176.

[7] Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. IEEE Access 2018, 6, 35365–35381

[8] Denning, D.E. An intrusion-detection model. IEEE Trans. Softw. Eng. 1987, 222–232

[9] M. Esposito, C. Mazzariello1, F. Oliviero1, S.P. Romano1 and C. Sansone, Evaluating Pattern Recognition Techniques in Intrusion Detection Systems, University of Napoli Federico II Dipartimento di Informatica e Sistemistica Via Claudio 21 — 80125 Napoli, Italy

[10] Heng Liao, Jiajin Tu, Jing Xia, Xiping Zhou, A Scalable Architecture for Neural Network Computing, 2019 IEEE Hot Chips 31 Symposium (HCS).

[11] Chaodong Tong, Learning Discriminative Text Representation for Streaming Social Event Detection, Second research room, Institute of Information Engineering CAS, 306628 Beijing, Beijing, China, 100093

[12] Syarif, A.R.; Gata, W. Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm. In Proceedings of the 2017 11th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, 31 October 2017; pp. 181–186

[13] Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. IEEE network, 8(3), 26-41

[14] Staudemeyer, R. C. (2015). Applying long short-term memory recurrent neural networks to intrusion detection. South African Computer Journal, 56(1), 136-154.

[16] Shah, R.; Qian, Y.; Kumar, D.; Ali, M.; Alvi, M. Network intrusion detection through discriminative feature selection by using sparse logistic regression. Future Internet 2017, 9, 81

[17] Luca Didaci, Giorgio Giacinto and Fabio Roli, Ensemble Learning for Intrusion Detection in Computer Networks, ACADEMIA, 2017

[18] T. Shibahara, T. Yagi, M. Akiyama, D. Chiba, and T. Yada, “Efficient dynamic malware analysis based on network behavior sing deep learning,” in Global Communications Conference (GLOBECOM), 2016 IEEE. IEEE, 2016, pp. 1–7

[19] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, “An empirical comparison of botnet detection methods,” computers & security, vol. 45, pp. 100–123, 2014

[20] G. Meena and R. R. Choudhary, “A review paper on ids classification using kdd 99 and nsl kdd dataset in weka,” in Computer, Communica tions and Electronics (Comptelix), 2017 International Conference on. IEEE, 2017, pp. 553–558