REVIEW ARTICLE

SAMRIDDHI Volume 15, Issue 1, 2023 Print ISSN: 2229-7111 Online ISSN: 2454-5767

A Comparative Study on Deep Learning-Based Algorithms For Intruder Detection Systems and Cyber Security

Vineeta Shrivastava, Megha Kamble

School of CST, LNCT UNIVERSITY, Bhopal, Madhya Pradesh, India.

Abstract

For data protection, the most vital factors are the statistics' safety, use of cryptographic controls during data transmission, an effective access management system, and powerful tracking. This paper seeks to provide a committed evaluation of the very current studies works on using Deep studying strategies to remedy computer security demanding situations. In this study, we analyzed and reviewed using deep learning algorithms for the Intruder detection system and Cybersecurity programs. Deep learning consists of system-mastering strategies that permit the network to learn from unsupervised data and solve complicated problems. Deep learning approaches such as Convolutional Neural Network (CNN), Auto Encoder (AE), Deep Belief Network (DBN), Recurrent Neural Network (RNN), Generative Adversal Network (GAN), and Deep Reinforcement Learning (DIL) are used to categorize the papers referred. This paper discusses various challenges, issues, and types of cyber-attacks and security measures.

Keywords: keywords Cybersecurity, Deep learning, supervised and unsupervised, Machine learning. Intrusion detection,.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2023); DOI: 10.18090/samriddhi.v15i01.30

Introduction

The enormous growth of the processer systems and their novel rising programs consume allowed the invaders to present diverse safety attacks beside them via various methods. Figure 1 shows the part of the safety assaults collected from McAfee Labs in 2017, wherein the maximum of them are browser assaults, brute force assaults, and allotted Denial of service (DDoS) attacks. Other than that, protection assaults for Wireless frame location networks (WBANS), fog computing, cellular computing, cloud computing, cellular ad-hoc networks, and SDNs are conducted. Intrusion detection structures are crucial safety components utilized in aggregate with firewalls to make the pc networks more stable locations for proudly owning IT businesses and their customers. IDS answers are one of the key protection components that, during aggregate with firewalls, can efficaciously manipulate several kinds of protection assaults.[1] IDS schemes can be specifically categorized as misuse detection schemes and anomaly detection schemes, which may be found out via way of means of the usage of various system learning strategies. Misuse detection or signature-primarily based totally structures intently depend on the signature of the safety assaults and malicious behaviors and manually the multi-beauty class. But, they cannot come upon the latest assaults in which their signature isn't always available for the IDS. But, as an advantage, the ones schemes advantage greater accuracy in recognizing identified malicious behaviors and their variations. On the alternative hand, ambiguity detection-based IDS strategies can come across new assaults thru relying on the users' regular behavior profiles and maximum efficacious aid binary classifications.[2]

A massive variety of recent studies is done in every anomaly detection and misuse detection context the usage of diverse tool gaining knowledge of strategies. Traditional device mastering strategies to be troubled via way of the dearth of categorised schooling datasets and carefully rely on the extracted functions via a human, making it difficult to deploy on massive structures. Deep gaining knowledge of is a singular paradigm withinside the device gaining knowledge of area mainly installed the use of ANNs or synthetic neural

Corresponding Author: Vineeta Shrivastava, Department of computer science & Engineering, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, India., e-mail: Shrivastavavinita21@gmail.com

How to cite this article: Shrivastava, V., Kamble, M. (2023). A Comparative Study on Deep Learning-Based Algorithms For Intruder Detection Systems and Cyber Security. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology,* 15(1), 154-160.

Source of support: Nil

Conflict of interest: None

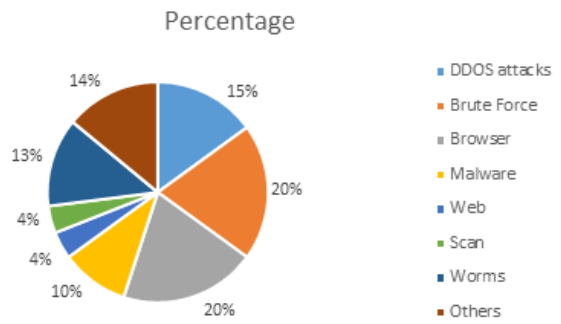

Figure 1: Types of security attacks in Mac free network in 2017.

networks and has a better overall performance than the alternative conventional gadget gaining knowledge of strategies.[3] Deep green people can extract higher representations from the uncooked records to create a lot higher models. Deep freshmen can studies higher because of the truth they are composed of more than one hidden layers.[4] At each layer, the version can extract a higher illustration from the characteristic set simultaneously in contrast to shallow freshmen who don't have hidden layers.[5]

Growing internet utilization has moreover introduced many protection gaps. Many technology, firewall, information encryption, and person authentication, are used to save you protection gaps. These protection mechanisms prevent many kinds of attacks.[7-8] However, that protection generation cannot perform in-depth packet evaluation. For that reason, they can't attain the popular level of assault detection. Intrusion Prevention gadgets (IPS) and IDS structures have been superior in complementing the shortcomings of those protection mechanisms.[9] These structures can carry out deeper statistics evaluation in assessment to extraordinary protection structures way to their algorithms which consist of device learning, deep gaining expertise of, and synthetic intelligence.[10-12] While IPS systems art work as each intrusion detection and prevention mechanism, IDS structures are used maximum successfully for intrusion detection and evaluation. On this examination, we centered on IDS structures.[13] Network protection may be attained the use of using a software program software utility referred to as an Intrusion Detection System (IDS) that allows withstanding network breaches.[14] The intention of these structures is to have a defended wall that stops such forms of assault. It identifies the illegal sports of a community or a laptop device.[15-16] Commonly, there are number one classes of IDS, specifically Anomaly detection and misuse detection. The former learns from recorded regular conduct to understand new intrusion attacks.[17] Any variance from contemporary baseline styles is determined as assaults and alarms are induced. Even aleven though misuse detection detects the intrusion primarily based totally at the repository of attacks signatures however has no faux alarm.[18] Deep gaining knowledge was inspired by way of the structure and depth of the human mind. Because of a couple of stages of abstraction, the network learns to map

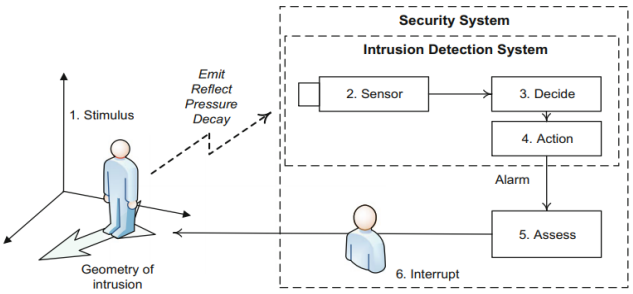

Figure 2: The Principle of Detection (Sarker, Colman, et al., 2020)

the enter capabilities to the output. The technique of gaining information does no longer depend upon human-crafted features.[19-20] Given a fixed of situations, the device can use a series of mathematical techniques to decide if a class is correct primarily based totally at the risk of error. Within the world of deep attending to know, we focus on deep networks wherein the type schooling is conducted via way of schooling with many layers in hierarchical networks with unsupervised mastering. Deep network intrusion detection systems may be categorized primarily based totally mostly on how the architectures and techniques have become used.[21]

Principle of Intrusion Detection

The detection precept is primarily based totally on the usage of sensor era to locate and react to the presence of someone or item in a described visible field. All computerized structures consist of additives for recording, processing (decision) and output (action). Figure 2 illustrates how IDS is perceived as a result of confusion in a person or thing. The schematic instance of Figure 1. three indicates how an IDS is detected because of an anomaly in an man or woman or item. The presence of someone or an item triggers the stimulus. Energy, including infrared radiation, a contemplated pulse, microwave radiation, a strain wave, or a molecular decay, might also be used as triggers. A like-minded stimulus triggers the sensor's response. There are a number of detectors available, starting from a passive infrared detector that searches for emitted infrared radiation to a lively micro-detector this is tuned to the frequency of glass breaks. A displaced Doppler wave is obtained with the aid of using waves. A threshold is used to determine whether or not an alarm has been caused that shows an atypical stimulus.

Intrusion detection systems (IDS) are part of the second one protection line of a gadget. IDSs can be deployed along with exceptional protection features, consisting of getting admission to manipulation, authentication mechanisms, and encryption techniques to better stabilize the systems in opposition to cyber-attacks.[22-23] The utilization of forms of benign web website online site visitors or regular behavior or specific regulations that describe a selected assault, IDSs can distinguish amongst normal and malicious moves. According to, information mining this is used to explain know-how discovery can assist in positioning into impact and installation

Table 1: Comparison table of various techniques for IDS and Cybersecurity

Ref	*Technique Used*	*Dataset*	*Accuracy*	*Recall*	*Precision*	*Fl-Score*	*Limitations*
Ref	ML-based	NSL-KDD	98%	0.94	0.90	0.94	Not good for the large data set
(Sarker, Colman, et al., 2020)	HMM based on ML	CSE-CIC-IDS	98.22%	0.99	0.93	0.98	High training time needed
(Zegeye et al., 2019)	ML-based	UNSW-NB15.	99.94%	-	0.75	-	Not good for the large data set
(Ashraf et al., 2022)	ML-based	KDD-CUP 99	98.39%	-	0.65	-	High training time needed
(R. Zhang et al., 2022)	SCADA	NSL-KDD	99.8%	0.1	0.98	0.99	Optimization for unknown pattern discovery
(Atul et al., 2021)	EASH framework based on ML	NSL-KDD	85%	0.79	0.96	0.74	Low dimensional data cause errors
(Lee et al., 2018)	Recurrent Neural Network	NSL-KDD	98.9 %	0.79	0.63	0.70	Multi-class problem is not handled

IDSs with better accuracy and strong conduct as compared to conventional IDSs that won't be as powerful in opposition to current brand new cyber-attacks.[24]

Our Contribution on this Work

- We first highlight the importance of protection capabilities for excessive dimensions in a device studying-based intrusion detection system.
- We review the intrusion detection systems that use deep learning methods.
- We examine 5 deep gaining knowledge of facts consistent with (i) recurrent neural networks, (ii) deep neural networks, and (iii) convolutional neural networks.

The remaining paper is prepared as follows. In phase II, we offer an overview of the Literature review. Phase III gives the intrusion detection structures based on deep getting to know procedures. In Phase IV, we present five deep studying methods. In phase V, we look at the overall performance of each deep gaining knowledge of approach the use of type. Lastly, Phase VI provides conclusions.

Literature Review

Within the area of cybersecurity, especially for detecting intrusions or cyber-attacks, numerous researchers used machine learning the kind techniques said above.

Iqbal H.et al[1] to discover numerous cyber-attacks or anomalies in a network and assemble an effective intrusion detection device proposed a model named Intrusion Detection Tree ("IntruDTree") device-mastering-primarily based totally safety model. The predicament of this paintings is that it does now no longer display effectiveness on huge datasets.

Li *et al.*[2] supplied an method to categorise the predefined assault instructions which includes DoS, Probe or scan, U2R, R2L, further to everyday traffic utilizing the most well-known KDD'99 cup dataset with the useful resource of using the hyperplane-primarily based totally aid vector device classifier with an RBF kernel.

Balogun *et al.*,[3] and Sangkatsanee *et al.* [4] used their studies' choice tree type method to assemble intrusion detection systems. But, with the immoderate dimensions of protection features, a desire tree version might also additionally purpose numerous issues, excessive variance with over-becoming, excessive computational charge and time, and coffee prediction accuracy.Sarker *et al.* [5] proposed currently, a behavioral decision tree set of rules is known as BehavDT for studying behavioral styles. The exceptionally acknowledged techniques for routinely building choice bushes are the ID3 and C4.5 algorithms. These days, a behavioral choice tree algorithm called BehavDT for studying behavioral patterns.

Alrowaily *et al.*[6] conducted several experiments on seven device mastering algorithms using the CICIDS2017 intrusion detection dataset.

Papamartzivanos *et al.*[7] The arrival of present-day assaults drives the industrial corporation and educational network to look at for particular procedures, which control to tightly hold song of this opposition and satisfactory-song swiftly to the alterations inside the subject

Zegeye *et al.*[8] proposed a machine gaining knowledge of multilayer hidden markov (HMM) version-based intrusion detection. The proposed gadget is famous for its excellent overall performance amongst all assessment metrics as 98% accuracy, 93% precision, 99.9% real, and 98 % F I-score.

Imran *et al.*[9] Propose an intrusion detection approach for the present-day network surroundings through thinking about the facts from satellites for computer and global networks. Incorporating machine getting to know fashions, the study proposes an ensemble version RFMLP that integrates random woodland (RF) and multilayer perceptron (MLP) for increasing

intrusion detection overall performance.

Shojafar *et al.*[10] An unsupervised studying the approach for intrusion detection has been designed to find clusters based totally on similarity supervised getting to know fashions want labels for training and display proper consequences.

Andresen *et al.*[11] Deep learning techniques to know models and deep hierarchical models Jiang *et al.*[12] have been proposed to research non-linear relationships of facts for malicious assault detection. ANN is applied at the KDD99 dataset for intrusion detection by the aid of lowering dimensions from correlation and statistics benefits. The version showed progressed results in positions of accuracy.

Abdulrahman *et al.*[13] Proposed a hybrid optimized long short-term memory (LSTM) to predict and identify network attacks in an IoT network. Firefly swarm optimization is integrated with LSTM to decrease the computational overhead, which in flip increases the prediction accuracy. Nearly 19,00,503 actual-time normal and attack data had been collected from the experimental simulation setup primarily based on the OMNET++ – Python – IoT framework.

Ruohao *et al.*[14] Proposed an algorithm called AMDES (unmanned aerial system multifractal analysis intrusion detection system) for spoofing attack detection based on wavelet leader multifractal analysis (WLM) and machine learning (ML). The ideal attains correctness of 98.58%.

Zhang *et al.*[15] Present an exciting implementation of deep getting to know Networks along with a trainer–scholar network structure, which indicates promising perspectives for implementation in a cell environment. The proposed community is lightweight, allowing it to be incorporated right into a low-electricity platform, along with a UAV, whilst performing accurate traffic photo classification.

Ashraf *et al.*[16] present an intensive and current review of the modern-day IoT-related IDS. And also offer a complete creation to the systems of modern IoT structures. The demanding situations and corresponding IDS research are offered.

Aldweesh *et al.*[17] reviewed the current improvements in deep getting to know-based IDS and offer a clear evaluation of an expansion of deep-gaining knowledge of-based IDS of differing taxonomies. Their article is an incredible manual for popular deep-gaining knowledge of algorithms for IDS.

X. Zhou *et al.*[18] propose a technique to solve the huge economic statistics anomaly detection problem by way of applying a variation LSTM (VLSTM) framework, which incorporates an LSTM-based encoder-decoder structure The VLSTM framework allows for the extraction of a selection of capabilities, and as a result lets in for the detection of diverse styles of anomalies.

Kushinagar *et al.*[19] propose a technique choice technique (EFFST) to achieve a substantial characteristic subset for internet attack detection using choosing a one-fourth split of the ranked capabilities. The experimentation at the CICIDS 2017 dataset indicates that the proposed EFFST method offers a detection fee of 99.09%, with J48 the usage of 24 functions.

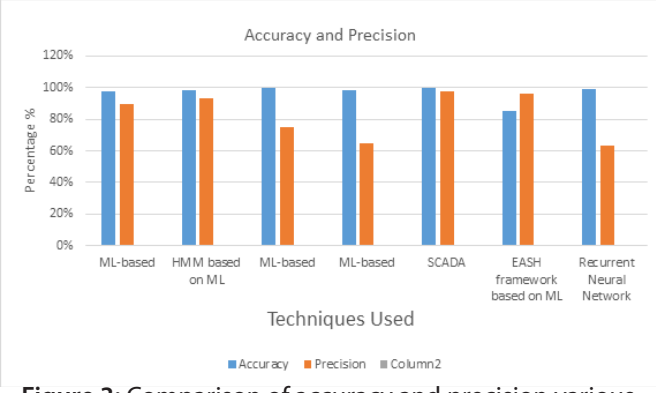

Figure 3: Comparison of accuracy and precision various techniques

Wu Wang *et al.*[20] proposed a technique to find out malicious assaults centered on SCADA structures. Specially, we look at the feasibility of a deep reading method for intrusion detection in SCADA structures the check additionally confirmed that the proposed approach outperformed the standalone deep reading fashions.

Yang *et al.*[21] brought a manner for assessing oil and fuel line SCADA protection thru the usage of causality assessment. This method followed the causality evaluation approach of fuzzy common sense reasoning for assessing factors neurons within the introduced method. It's been demonstrated that the causality evaluation-pushed approach offers actual cap potential in assessing SCADA records protection.

Pan, Z *et al.*[22] brought an intrusion detector that's primarily based totally at the idea of Context Awareness and Anomaly Behavior Analysis (ABA), to discover and classify distinctive kinds of assaults in the building automation and Control community (BACnet).

Linda *et al.*[23] proposed an anomaly detection scheme based totally on neural networks. They exploited the SCADA community and gadget records to deal with the trouble of awful packets. However, this answer can handiest cope with outside assaults; the inner attackers can nonetheless introduce malicious command packets to contaminate important equipment.

Basnet *et al.*[24] proposed a deep studying-based intrusion detection system (IDS) to detect the denial of carrier (DoS) assaults inside the EVCS. The deep neural community (DNN) and long-quick period memory (LSTM) algorithms are carried out.

Gottumukkala *et al.*[25] Supervisory control and data acquisition (SCADA) gadgets, inner sensors, and electric-powered cars (EVs) through the net to make certain energy performance and availability. Permitting wireless technology might be wireless, cell, or Bluetooth.

Thanks, J you *et al.*[26] Recommend strength conscious smart home (EASH) framework to remedy the trouble in communication failures and types of network attacks are analyzed in EASH. The classical attains correctness of 85%.

Rahman *et al.*[27] proposed a new technology based totally on the IDS machine of the Internet of Things (IoT). To transmit

the processing paintings, they improve comparable person models of learning that correspond to a shared set of pressure records. In mild of similar research of work whilst clarifying the mathematical outcomes and the rundown of proposed techniques, supply SDI detection exactness corresponding to senior facilities, and shows the inherent barriers among accuracy and creation time

Wenjuan Li *et al.*[28] studied semi-supervised studying and designed DAS-CIDS by way of making use of disagreement-based semi-supervised gaining knowledge of a set of rules to the CIDS system. The investigational consequences presented that their method became more effective than conventional supervised classifiers at detecting intruders and lowering fake positives using unlabelled records.

Daming Li *et al.*[29] proposed IoT extraction highlights and interruption popularity algorithms for the motion-primarily based intelligent city within the learning version joins the profundity version of interruption location innovation with learning.

The Table 1 shows comparison of various techniques for IDS and cybersecurity

The comparison of accuracy and precision for various techniques is shown in Figure 3.

Types of Attacks

- Active attacker: These invaders produce false messages and can stop promoting the conventional despatch.
- Passive attacker: These invaders lone overhear on the wireless network, gathering traffic data and advancing it to other assailants.
- Inside attacker: These invaders can have whole information of the system formation; therefore, these types of attackers are very hazardous as associated to extra invaders.
- Outsider Attacker: These invaders are not being authenticated and are less hazardous than insider attackers.
- Malicious Attacker: These invaders have attempted to forcefully abuse or take advantage of network data, and mainly harm other nodes. They can strictly destroy the network.
- Rational Attacker: These invaders damage the network for their own profit and can be effortlessly traced.
- Local Attackers: These invaders can execute only to a slight area.
- Extended Attackers: These attackers have a broad range and can attack through the network.
- Web Attack: Web disfigurement is an assault wherein noxious gatherings infiltrate a site and supplant website content with their messages.
- Botnet Attack: A botnet is an assortment of associated web gadgets, which might incorporate (PCs), servers, cell phones and web of things (IoT) gadgets, that are tainted and constrained by a typical kind of malware, frequently unbeknownst to their proprietor.
- Heartbleed Attack: The Heartbleed Bug is a not kidding weakness in the well-known OpenSSL cryptographic programming library. This shortcoming permits taking the data safeguarded, under typical circumstances, by the SSL/TLS encryption used to get the Internet.
- Brute Force Attack:- A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.
- DDoS Attack: The DDoS assault will send various solicitations to the went-after web asset - determined to surpass the site's ability to deal with numerous solicitations… and keep the site from working accurately. Run of the mill focuses for DDoS assaults include Internet shopping locales.
- DoS Attack: A denial-of-service (DoS) attack is meant to shut down a machine or network, making it inaccessible to its intended users.

Overview of Deep Learning Techniques

This section presents an in-depth overview of the various in-depth learning and machine learning supervised algorithms and outlines the requirements for developing in-depth learning algorithms in many areas such as IDS. The implications for the continuous development of modern technology create the need for machine learning algorithms to become increasingly needed for extracting and analyzing information on a large number of created databases. In this paper, our interest is based on the following machine learning algorithms; because the CICIDS2017 target data set contains pre-defined classes.

Adaptive Boosting (AdaBoost) a development method, a machine learning algorithm designed to improve the efficiency of categories. The basic working concept of developing algorithms can be defined as follows; groups first sort data with draft rules. New rules are given to these unfinished rules whenever an algorithm is used. In this way, a few weak and less effective rules are found called "basic rules".

Multilayer perceptron (MLP) a category of sensory networks (ANN). ANN is a machine-learning mechanism that inspires the way the human brain works. This approach aims to mimic the human brain's features, for example, by making decisions and acquiring new knowledge. Although the human brain consists of interconnected nerve cells, the ANN contains synthetic connective cells.

Decision Tree (DT) is an identical influential instrument for classification and prediction. The Deciduous Tree is a flowing drawing like a tree structure, in which each tree includes leaves, branches, and nodes. It divides the database into subdivision sets while at the same time the associated decision tree is increasingly constructed. The end result is a tree with buds and leaves.

Naive Bayes (NB) is a family classification strategy that is likely to benefit from the theory of opportunity and the Bayes theory of predictable modeling, which assumes that all factors are statistically independent. It calculates the probability of each element in order to select the most likely

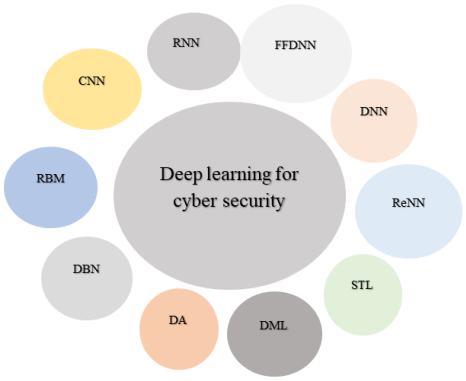

Figure 4: Deep learning techniques for cyber security

outcome. Effectiveness of Electronic Learning Processing Systems 285

K-Neighborhood Neighborhood (KNN) is a flexible and sample-based approach. Depending on how the data points are divided into multiple classes, in other words, the same objects are closer to each other to determine the closest neighbors to K.

Quadratic Discriminant Analysis (QDA) a discriminatory analysis method used to identify which differences distinguish between two or more groups occur naturally; it may have a predictive or descriptive goal.

Random Forest (RF) a machine learning method that uses cutting trees. In this way, the "forest" is produced by combining a large number of deciduous tree structures.

Deep learning approaches used for cyber security intrusion detection

Deep neural network (DNN) Deep neural network (DNN) is an artificial neural network (ANN) with multiple layers between input and output. Figure 4 shows deep learning techniques for cyber security.

Convolutional neural network (CNN) is a class of deep emotional networks widely used to analyze visual images.

Recurrent neural network (RNN) Recurrent neural network (RNN) is a special type of artificial neural network that is converted to process time data or sequence data.

Replicator Neural Network (ReNN) Replicator neural networks compress data with a hidden layer using a step-by-step activation function.

Feed-forward deep neural network (FFDNN) they are models for deep critical learning. The goal of the feedforward network is to measure a certain function f *. For example, in the case of a divider, y = f * (x) sets the input x in the y.

Deep belief network (DBN) used to solve unsupervised learning activities to reduce the size of the features, and can be used to solve supervised learning activities to create subdivision models or retrospective models.

Restricted Boltzmann machine (RBM) Boltzmann Restricted machine is a useful algorithm for reducing size, partition, and rotation, shared filtering, feature reading, and title modeling.

Deep auto-encoder (DA) aims to copy their input into their results. They work by pressing input into a hidden location representation and then re-creating the output from this representation.

DML Deep migration learning.

STL SelfTaught Learning.

Conclusion

The object is to offer a dedicated review of this recent research works using Deep Learning strategies to solve computer security challenges. In this comparison, we detected that the Machine learning-based ensemble version RFMLP model achieves 99.94% accuracy which is the highest compared to other IDS and cyber security techniques. However, the major consideration is to identify the best technique that can be functional to any ideal, in order to growth the performance of the model and protect our data from hackers.

References

[1] Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 105124. https://doi.org/https://doi.org/10.1016/j.knosys.2019.105124

[2] Alqahtani, A. S. (2022). FSO-LSTM IDS: hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks. The Journal of Supercomputing. https://doi.org/10.1007/s11227-021-04285-3

[3] Alrowaily, M. (2020). Investigation of Machine Learning Algorithms for Intrusion Detection System in Cybersecurity. [Digital Commons @ University of South Florida].

[4] Andresini, G., Appice, A., Mauro, N. Di, Loglisci, C., & Malerba, D. (2020). Multi-Channel Deep Feature Learning for Intrusion Detection. IEEE Access, 8, 53346–53359. https://doi.org/10.1109/ACCESS.2020.2980937

[5] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. Electronics, 9(7). https://doi.org/10.3390/electronics9071177

[6] Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F., & Rasool, N. (2022). A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection. Electronics, 11(4). https://doi.org/10.3390/electronics11040667

[7] Atul, D. J., Kamalraj, R., Ramesh, G., Sakthidasan Sankaran, K., Sharma, S., & Khasim, S. (2021). A machine learning based IoT for providing an intrusion detection system for security. Microprocessors and Microsystems, 82, 103741. https://doi.org/https://doi.org/10.1016/j.micpro.2020.103741

[8] Basnet, M., & Hasan Ali, M. (2020). Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station. 2020 2nd International Conference on Smart Power Internet Energy Systems (SPIES), 408–413. https://doi.org/10.1109/SPIES48661.2020.9243152

[9] Choi, Y.-H., Liu, P., Shang, Z., Wang, H., Wang, Z., Zhang, L., Zhou, J., & Zou, Q. (2020). Using deep learning to solve computer security challenges: a survey. Cybersecurity, 3(1), 15. https://doi.org/10.1186/s42400-020-00055-5

[10] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/https://doi.org/10.1016/j.jisa.2019.102419

[11] Gottumukkala, R., Merchant, R., Tauzin, A., Leon, K., Roche, A., & Darby, P. (2019). Cyber-physical System Security of Vehicle Charging Stations. 2019 IEEE Green Technologies Conference(GreenTech), 1–5. https://doi.org/10.1109/GreenTech.2019.8767141

[12] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network. IEEE Access, 8, 32464–32476. https://doi.org/10.1109/ACCESS.2020.2973730

[13] Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188, 107840. https://doi.org/https://doi.org/10.1016/j.comnet.2021.107840

[14] Kshirsagar, D., & Kumar, S. (2022). Towards an intrusion detection system for detecting web attacks based on an ensemble of filter feature selection techniques. Cyber-Physical Systems, 0(0), 1–16. https://doi.org/10.1080/23335777.2021.2023651

[15] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., Hosseinzadeh, M., & Rahmani, A. M. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, 9, 101574–101599. https://doi.org/10.1109/ACCESS.2021.3097247

[16] Lee, B., Amaresh, S., Green, C., Engels, D., & Engels, D. W. (2018). SMU Data Science Review Comparative Study of Deep Learning Models for Network Intrusion Detection Comparative Study of Deep Learning Models for Network Intrusion Detection. Other Computer Engineering Commons, Other Computer Sciences SMU Data Science Review, 1(1). https://scholar.smu.edu/datasciencereviewAvailableat:https://scholar.smu.edu/datasciencereview/vol1/iss1/8

[17] Li, D., Deng, L., Lee, M., & Wang, H. (2019). IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. International Journal of Information Management, 49, 533–545. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.04.006

[18] Li, W., Meng, W., & Au, M. H. (2020). Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications, 161, 102631. https://doi.org/https://doi.org/10.1016/j.jnca.2020.102631

[19] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Systems with Applications, 39(1), 424–430. https://doi.org/https://doi.org/10.1016/j.eswa.2011.07.032

[20] Linda, O., Vollmer, T., & Manic, M. (2009). Neural Network based Intrusion Detection System for critical infrastructures. 2009 International Joint Conference on Neural Networks, 1827–1834. https://doi.org/10.1109/IJCNN.2009.5178592

[21] Network Intrusion Detection | Kaggle. (n.d.). Retrieved January 24, 2023, from https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection

[22] Pan, Z., Pacheco, J., Hariri, S., Chen, Y., & Liu, B. (2019). Context Aware Anomaly Behavior Analysis for Smart Home Systems. 13(5), 261–274. http://waset.org/publications/10010351/pdf

[23] Papamartzivanos, D., Gomez Marmol, F., & Kambourakis, G. (2019). Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems. IEEE Access, 7(c), 13546–13560. https://doi.org/10.1109/ACCESS.2019.2893871

[24] Rahman, M. A., Asyhari, T., Leong, L. S., Satrya, G., Tao, M., & Zolkipli, M. (2020). Scalable Machine Learning-Based Intrusion Detection System for IoT-Enabled Smart Cities. Sustainable Cities and Society, 61, 102324. https://doi.org/10.1016/j.scs.2020.102324

[25] Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2011). Practical real-time intrusion detection using machine learning approaches. Computer Communications, 34(18), 2227–2235. https://doi.org/https://doi.org/10.1016/j.comcom.2011.07.001

[26] Sarker, I. H., Colman, A., Han, J., Khan, A. I., Abushark, Y. B., & Salah, K. (2020). BehavDT: A Behavioral Decision Tree Learning to Build User-Centric Context-Aware Predictive Model. Mobile Networks and Applications, 25(3), 1151–1161. https://doi.org/10.1007/s11036-019-01443-z

[27] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry, 12(5). https://doi.org/10.3390/sym12050754

[28] Shojafar, M., Taheri, R., Pooranian, Z., Javidan, R., Miri, A., & Jararweh, Y. (2019). Automatic Clustering of Attacks in Intrusion Detection Systems. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), 1–8. https://doi.org/10.1109/AICCSA47632.2019.9035238

[29] Tertytchny, G., Nicolaou, N., & Michael, M. K. (2020). Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning. Microprocessors and Microsystems, 77, 103121. https://doi.org/https://doi.org/10.1016/j.micpro.2020.103121

[30] Wang, W., Harrou, F., Bouyeddou, B., Senouci, S.-M., & Sun, Y. (2022). A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. Cluster Computing, 25(1), 561–578. https://doi.org/10.1007/s10586-021-03426-w

[31] Yang, L., Cao, X., & Geng, X. (2019). A novel intelligent assessment method for SCADA information security risk based on causality analysis. Cluster Computing, 22(3), 5491–5503. https://doi.org/10.1007/s10586-017-1315-4

[32] Zegeye, W. K., Dean, R. A., & Moazzami, F. (2019). Multi-Layer Hidden Markov Model Based Intrusion Detection System. Machine Learning and Knowledge Extraction, 1(1), 265–286. https://doi.org/10.3390/make1010017

[33] Zhang, J., Wang, W., Lu, C., Wang, J., & Sangaiah, A. K. (2020). Lightweight deep network for traffic sign classification. Annals of Telecommunications, 75(7), 369–379. https://doi.org/10.1007/s12243-019-00731-9

[34] Zhang, R., Condomines, J.-P., & Lochin, E. (2022). A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System. Drones, 6(1). https://doi.org/10.3390/drones6010021

[35] Zhou, X., Hu, Y., Liang, W., Ma, J., & Jin, Q. (2021). Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. IEEE Transactions on Industrial Informatics, 17(5), 3469–3477. https://doi.org/10.1109/TII.2020.3022432