International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR CYBERSECURIY

V.Swathi, Professor, Department Of CS SICET, Hyderabad

Mudavath Neeraja, Sahaja Burugu, Rallagudem Nikitha Reddy, Sama Kranthi Kumar Goud

UG Student, Department Of CS, SICET, Hyderabad

ABSTRACT

The rapid growth and development of the Internet in recent years has led to increased exposur e to cyber attacks and changes. Therefore, good access research is needed to protect data, and discoveries in the subfields of artificial intelligence, machine learning and deep learning are one of the best ways to solve this problem. This article reviews intrusion detection systems an d discusses the types of machine learning and deep learning learning algorithms used to prote ct data from malicious behavior. It discusses various networking applications, applications, al gorithms, learning, and data, as well as the latest machine learning and deep learning techniq ues to create functional access to search. , deep learning, intrusion detection system.

I. Introduction

The Internet today is changing people's work, education and lifestyle, living together with the Internet and therefore increasing the number of threats. It is now important to learn how to id entify cyber threats and cyber attacks, especially cyber attacks you have seen before. Cyberse curity is defined as the process of using network protection and policies to protect data, progr ams, servers, and network infrastructure from unauthorized access or modification. The Inter net connects most of our computer systems and network infrastructure. Therefore, cybersecur ity has become fundamental for almost every company, government, and even individual to p rotect their information, grow their business, and govern themselves. and manipulation. Incre asing internet usage has increased the volume and complexity of data, which has led to the e mergence of big data. The rise of the internet and public information should lead to a better u nderstanding of search engines. Network security is the part of network security that protects

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

networked systems from malicious attacks. The goal is to provide reliabledata security, integr ity and easy access to connected computers. Cybersecurity research is currently focused on de veloping effective insights that can identify known and new attacks and threats with high acc uracy and low latency [1].

alarm rate [1].

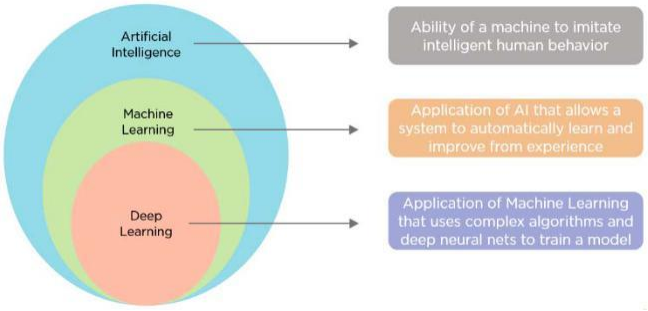


FIGURE 1. Relation between Artificial Intelligence, Machine Learning, and Deep Learning

A. Halbouni et al.: ML and DL approaches to cybersecurity: A review of the best q uestion. Deep learning is a subfield of machine learning, which is a subfield of artif icial intelligence. Therefore, machine learning and deep learning are used to provid e efficient and effective access to search. This article focuses on network security te chnologies, methods, and applications and provides an overview of machine learnin g, deep learning, and access discovery techniques. This is a way for computers to m ake rules about how they should display data, rather than allowing humans to do so. Machine learning algorithms are algorithms that can learn and adapt based on data. Machine learning algorithms are designed to produce output based on information learned from data and examples. For example, such algorithms will allow computer s to select and perform specific tasks without detailed information to search for new tools [2]. Media analysis and attack detection can be done effectively using machin e learning [1]. As shown in Figure 2, there are three main types of machine learning : supervised learning, unsupervised learning, semisupervised learning, and increme ntal learning. Supervised learning is based on recorded data, unsupervised learning is based on anonymous data and semi-supervised learning is based on both.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

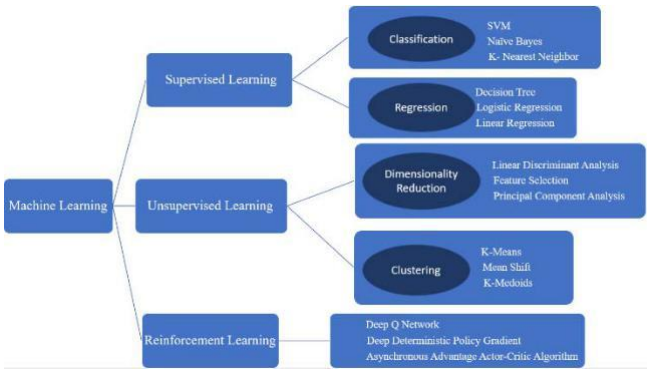
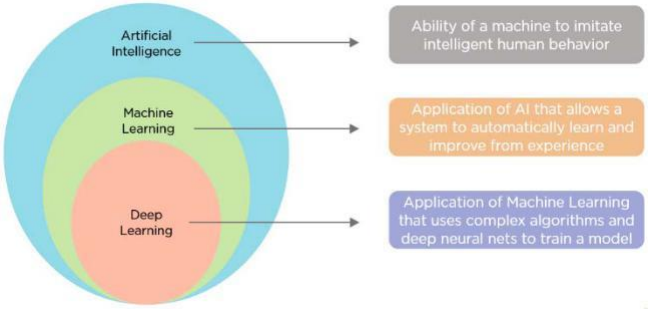


Figure 2. Machine learning methods and algorithms

Deep learning (DL) is a new subfield of machine learning and its own subfield of artificial int elligence (AI). Traditional machine learning methods are limited to natural raw data processi ng based on extracting sufficient features, and to identify or discover patterns from distribute d raw data, it must be transformed into the appropriate model, which is deep learning. A mac hine learning method that can learn from unstructured or anonymous data and representations based on human brain knowledge [3]. Perform analysis and learning by analyzing data such as text, images, and audio by following the human brain [4]. Compared to multilayer deep learning mo dels, shallow learning models have fewer hidden la yers. By stacking layers upon layers, deep learning can work to make things more complex. Deep learn ing is used to learn language representations with d ifferent levels of abstraction



Deep Learning IDS Algorithms

This section discusses recent applications of DLIDS using various deep learning methods. [2 4] introduced a model that uses their data to collect and label real traffic connections to study mobile application identification and connectivity to cloud servers. Deep learning methods su ch as AE, CNN, and RNN were used to learn the classification, and the best performance was obtained from CNN and LSTM, achieving 91.8% accuracy for CNN classification and 90.1

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

% accuracy for Fmeasurement. However, their analysis is limited to specific applications, and since all features are equally important, CNNs and RNNs cannot evaluate the importance wh en obtaining the character of features. > [25] Combine deep learning with network virtualizati on to identify malicious behavior of IoT networks. Their technology enables effective detecti on of potential and interoperability in IoT networks by simulating and tracking five different attacks. Their model achieved 95% sensitivity and 97% recall for a wide range of risk factors. But like many other IDS models, they emphasize detection rather than prevention. Figure 8 s hows the implementation of the IDS deep learning model.

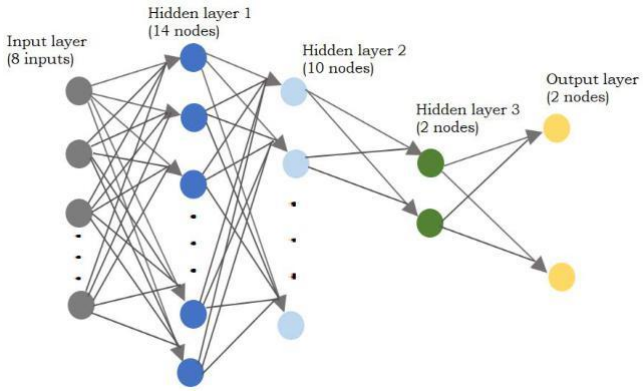


FIGURE 8. Sample of IDS deep learning model

CONCLUSION

One of the fundamental subjects in the field of cyber security has been intrusion detection systems. Many researchers are developing systems to secure data against malicious behavior. However, other applications of learning algorithms, such as creating a new data set or merging algorithms, are currently being researched. As a result, we explainconcept of intrusion detection system, types of attacks and how to find out whether we have an effective system or not in this work.Choosing a good dataset for training and testing an intrusion detection system is a key parameter and it was clear that datasets have an impact on research in the sector as some consider them outdated or contain redundant information. As a result, the research compares the most common datasets used for threat detection over the last decade.The last step in this project was to research what other people have done to save their data. Recent research has revealed that there are many implementations of data protection.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

First, they used machine learning for several purposes, and many studies were conducted to see which algorithm would provide higher accuracy or which datasets would produce lower false alarm rates. Finally, after extensive research and testing, they arrived at deep learning. Many studies and experiments have shown that deep learning is better than machine learning because it can handle more complicated problems with greater accuracy and lower false alarm rates. Previous works have been used in various applications. They used different datasets, architectures, learning methodologies and learning algorithms to secure data against attacks and dangers every time.

REFERENCE

[1] D. I. Edeh, "Network Intrusion Detection System using Deep Learning Technique", Master of Science, Department of Computing, University of Turku, 2021.

[2] G. C. Fernandez, “Deep Learning Approaches for Network Intrusion Detection,” Master of Science, The University of Texas at San Antonio, 2019.

[3] H. Benmeziane, “Comparison of Deep Learning Frameworks and Compilers”, Master in Computer Science, École nationale Supérieure d’Informatique, 2020.

[4] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/access.2018.2836950.

[5] I. Goodfellow, Y. Bengio and A. Courville, Deep learning. MIT Press, 2016.

[6] H. Dhillon, “Building Effective Network Security Frameworks using Deep Transfer Learning Techniques”, Master of Science, Western University, 2021.

[7] M. Labonne, “Anomaly based network intrusion detection using machine learning”, PhD, Institut Polytechnique de Paris, 2020.

[8] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of deep learning to real-time Web Intrusion detection," IEEE Access, vol. 8, pp. 70245-70261, 2020.

[9] P. Wu, “Deep Learning for Network Intrusion Detection: Attack Recognition with Computational Intelligence”, Master of Philosophy, School of Computer Science and Engineering, University of New South Wales, 2020.

[10] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network-based intrusion detection data sets,” Computers & Security, vol. 86, pp. 147-167, 2019.

[11] M. Alkasassbeh and M. Almseidin, “Machine Learning Methods for Network Intrusion Detection”, arXiv preprint arXiv:1809.02610, 2018.

12] T. Hamed, R. Dara, and S. C. Kremer, "A network intrusion detection system based on recursive feature addition and bigram technique," Computers & Security, vol. 73, pp. 137-155, 2018.