Deep Learning and Cyber Security

Prashant Chhonker, Mr. S.Ponmaniraj Asst. Prof.

Department of Computer Science and Engineering
School Of Computing Science And Engineering
Galgotias University

Abstract

Deep Learning(DL), a novel research direction in Machine Learning(ML) field has achieved a great success in many classical Artificial Intelligence(AI) tasks. DL architectures are relatively recent and currently wisely used for diverse Cyber Security applications.. Initially, the concepts of most popular ML algorithms and DL architectures are discussed along with the mathematical representations. Following, we review the emerging researches of DL architectures for diverse anticipated applications of Cyber Security. This include Intrusion detection, Malware and Botnet detection, Spam and Phishing detection, Network traffic analysis, Binary analysis, Insider threat detection, CAPTCHA analysis, steganography. Additionally, the importance of DL architectures are discussed for cryptography, cloud security, biometric security, smart cities specific to Internet of things (IoT) and fog computing. We discuss the importance of big data, natural language processing, signal and image processing, blockchain technology,casual theory key concepts towards Cyber Security. Cyber security is the collection of policies, techniques, technologies, and processes that work together to protect the confidentiality, integrity, and availability of computing resources, networks, software programs, and data from attack. Cyber defense mechanisms exist at the application, network, host, and data level. There is a plethora of tools—such as firewalls, antivirus software, intrusion detection systems (IDSs), and intrusion protection systems (IPSs)—that work in silos to prevent attacks and detect security breaches. However, many adversaries are still at an advantage because they only need to find one vulnerability in the systems needing protection. As the number of internet-connected systems increases, the attack surface also increases, leading to greater risk of attack. Furthermore, attackers are becoming more sophisticated, developing zero-day exploits and malware that evade security measures, enabling them to persist for long periods without notice. Zero-day exploits are attacks that have not been encountered previously but are often variations on a known attack. To exacerbate the problem, attack mechanisms are being commoditized, allowing for rapid distribution without needing an understanding for developing exploits. In addition to defending against external threats, defenders also must guard against insider threats from individuals or entities within an organization that misuse their authorized access. Throughout an attack’s lifecycle, there are indicators of compromise; there may even be significant signs of an impending attack. The challenge is in finding these indicators, which may be distributed across the environment. There are massive quantities of data from applications, servers, smart devices, and other cyber-enabled resources generated by machine-to-machine and human-to-machine interactions. Cyber defense systems are generating voluminous data, such as the Security Information Event Management (SIEM) system, which often overwhelms the security analyst with event alerts. The use of data science in cyber security can help to correlate events, identify patterns, and detect anomalous behavior to improve the security posture of any defense program. We are starting to see an emergence of cyber defense systems leveraging data analytics. For instance, network intrusion detection systems (NIDSs) that inspect packet transmissions are evolving from signature-based systems that detect well-known attacks to anomaly-based systems that detect deviations from a “normal” behavior profile.

1.Introduction

Cyber security is the collection of policies, techniques, technologies, and processes that work together to protect the confidentiality, integrity, and availability of computing resources, networks,

software programs, and data from attack. Cyber defense mechanisms exist at the application, network, host, and data level. There is a plethora of tools—such as firewalls, antivirus software, intrusion detection systems (IDSs), and intrusion protection systems (IPSs)—that work in silos to prevent attacks and detect security breaches. However, many adversaries are still at an advantage because they only need to find one vulnerability in the systems needing protection. As the number of internet-connected systems increases, the attack surface also increases, leading to greater risk of attack. Furthermore, attackers are becoming more sophisticated, developing zero-day exploits and malware that evade security measures, enabling them to persist for long periods without notice. Zero-day exploits are attacks that have not been encountered previously but are often variations on a known attack.

To exacerbate the problem, attack mechanisms are being commoditized, allowing for rapid distribution without needing an understanding for developing exploits. In addition to defending against external threats, defenders also must guard against insider threats from individuals or entities within an organization that misuse their authorized access. Throughout an attack's lifecycle, there are indicators of compromise; there may even be significant signs of an impending attack. The challenge is in finding these indicators, which may be distributed across the environment. There are massive quantities of data from applications, servers, smart devices, and other cyber-enabled resources generated by machine-to-machine and human-to-machine interactions. Cyber defense systems are generating voluminous data, such as the Security Information Event Management (SIEM) system, which often overwhelms the security analyst with event alerts. The use of data science in cyber security can help to correlate events, identify patterns, and detect anomalous behavior to improve the security posture of any defense program. We are starting to see an emergence of cyber defense systems leveraging data analytics. For instance, network intrusion detection systems (NIDSs) that inspect packet transmissions are evolving from signature-based systems that detect well-known attacks to anomaly-based systems that detect deviations from a "normal" behavior profile.

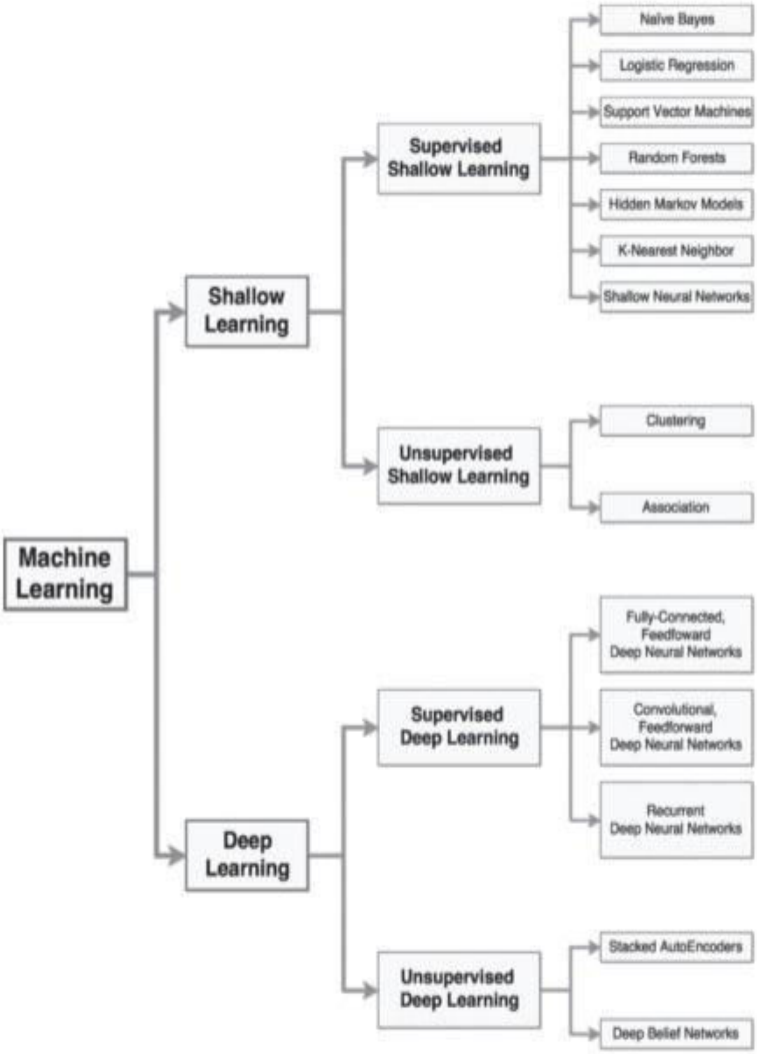
Cyber Security has become an important area of research due to the explosive growth in the number of attacks to the computers and networks. This contains a set of concepts and procedures to protect ICT systems and networks, both hardware and software from malicious software programs and more importantly data from unauthorized access, theft, disclosure, as well as intentional or accidental harm **.** Cyber Security evolves over time as the technology evolves to cope with the new types of patterns of malicious activity. To attack various threats, ID, social network security, malware analysis, advanced persistent threats, web application security, and applied cryptography, are few used tools in Cyber Security. However, even spam remains a major focus in an email system. This is also called as information technology security or elec-tronic security. More formally Cyber Security is defined by **,** the preservation of confidentiality, integrity and availability of information in the Cyberspace. Cyber Security is a broad terms and it includes information security, network security, Internet security, Critical information infrastructure protection, cyber crime, cyber safety and ICT security. Information security deals with protection of electronic data from unauthorized source.

2.Deep Learning Algorithms For Cyber Security

Deep learning includes a large variety of paradigms in continuous evolution, presenting weak boundaries and cross relationships. Furthermore, different views and applications may lead to different classifications. Hence, we cannot refer to one fully accepted taxonomy from literature, but we prefer to propose an original taxonomy able to capture the differences among the myriad of techniques that are being applied to cyber detection, as shown in Figure 1. This taxonomy is specifically oriented to security operators and avoids the ambitious goal

Learning (SL), in opposition to the more recent Deep Learning (DL). Shallow Learning requires a domain expert (that is, a feature engineer) who can perform the critical task of identifying the relevant data characteristics before executing the SL algorithm. Deep Learning relies on a multi-layered representation of the input data and can perform feature selection autonomously through a process defined representation learning.

FIGURE 1. CLASSIFICATION OF ML ALGORITHMS FOR CYBER SECURITY APPLICATIONS.



SL and DL approaches can be further characterized by distinguishing between supervised and unsupervised algorithms. The former techniques require a training process with a large and representative set of data that have been previously classified by a human expert or through other means. The latter approaches do not require a prelabelled training dataset. In this section, we consider and compare the most popular categories of ML algorithms, which appear as the leaves of the classification tree in. We remark that each category can include dozens of different techniques.

2.1 Shallow Learning vs Deep Learning

Artificial neural networks (ANNs) are machine learning algorithms inspired by the central nervous system. They were first conceived in 1943 when McCulloch and Pitt published a study presenting the mathematical model based on biological neuron. This was later implemented by Hebb and Rosenblatt in their development of unsupervised through self-organized learning and supervised learning through the creation of perceptrons, respectively. They are composed of a few layers of neurons connected by adaptive weights, and the adjacent network layers are usually fully connected. The universal approximation theorem for ANNs states that every continuous function that maps intervals of real numbers to some output interval of real numbers can be approximated arbitrarily closely by a multi-layer perceptron (type of ANN) with just one hidden layer. This means that an ANN with one hidden layer is capable of producing any non-linear continuous function, and as such much of the early research on ANNs concentrated on networks with just one hidden layer, trained using back-propagation . Networks with just one hidden layer belong to the category of shallow learning. There are unsupervised and supervised shallow network architectures. Supervised learning uses labels (ground truth) to learn a task; unsupervised learning is performing a machine learning task without labels. In shallow learning, feature extraction is performed separately, not as a part of the network.

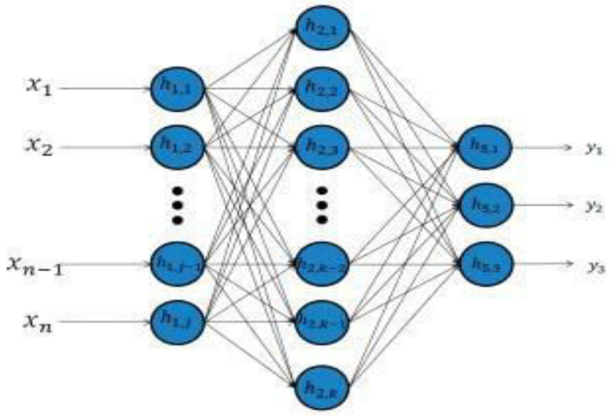


Figure2. Shallow Learning

DL is a much newer endeavor, with the first computer implementation achieved in 2006 .There are many definitions of DL and deep neural networks (DNNs). A simple definition states that DL is a set of machine learning algorithms that attempt to learn in multiple levels, corresponding to different levels of abstraction (Figure 3). The levels correspond to distinct levels of concepts, where higher-level concepts are defined from lower-level ones, and the same lower-level concepts can help to define many higher-level concepts . Feature extraction is performed by the first few layers of the deep network. There are unsupervised, supervised, and hybrid DL architectures. Because shallow neural networks have only one hidden layer, they lack the ability to perform advanced feature extraction and are unable to learn the higher-level concepts that deep neural networks are capable of learning. This also holds true for other machine learning algorithms, as well. However, DL methods require greater computational power, sometimes multiple graphical processing units (GPUs), to train DL models in a reasonable time. Two advancements have made it possible for an average person to easily develop DL models. The first is the increased availability of GPUs, which allow for significantly faster computation. The second is the fact that the layers with a DL model can be trained independently of each other . This means that a large model with millions of parameters can be optimized in small, manageable chunks, requiring significantly fewer resources. Information 2019, 10, x FOR PEER REVIEW 3 of 35 Figure 2. Shallow neural network. DL is a much newer endeavor, with the first computer implementation achieved in 2006 . There are many definitions of DL and deep neural networks (DNNs). A simple definition states that DL is a set of machine learning algorithms that attempt to learn in multiple levels, corresponding to different levels of abstraction (Figure 3). The levels correspond to distinct levels of concepts, where higher-level concepts are defined from lower-level ones, and the same lower-level concepts can help to define many higher-level concepts. Feature extraction is performed by the first few layers of the deep network. There are unsupervised, supervised, and hybrid DL architectures. Because shallow neural networks have only one hidden layer, they lack the ability to perform advanced feature extraction and are unable to learn the higher-level concepts that deep neural networks are capable of learning. This also holds true for other machine learning algorithms, as well. However, DL methods require greater computational power, sometimes multiple graphical processing units (GPUs), to train DL models in a reasonable time. Two advancements have made it possible for an average person to easily develop DL models. The first is the increased availability of GPUs, which allow for significantly faster computation. The second is the fact that the layers with a DL model can be trained independently of each other [16]. This means that a large model with millions of parameters can be optimized in small, manageable chunks, requiring significantly fewer resources.

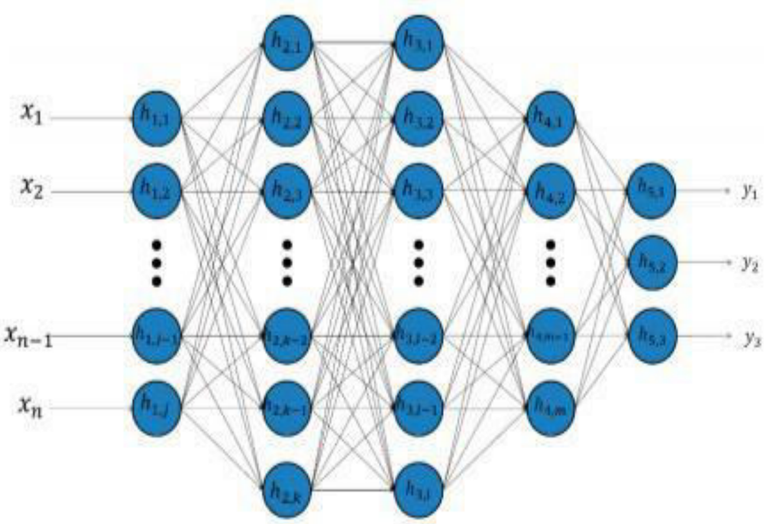


Figure3. Deep Learning

The main difference between Deep Learning and Shallow learning lies in the number of hidden layers. DL architectures have multiple hidden layers whereas shallow neural networks have at most one hidden layer.

3.Cyber Security

Security is becoming one of the most important topics in industrial IT and Operational Technology (OT), i.e. the hardware and software used in the production area. Cyber security is defined as technologies and processes constructed to protect computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through Internet by cyber criminals, terrorist groups and hackers. Cyber security is related to protecting your internet and network based digital equipments and information from unauthorized access and alteration. One of the most challenging elements of cyber security is the quickly and constantly evolving nature of security risks. The enterprise network comprised of mainframes, client-server model, closed group of systems and the attacks were very limited with viruses, worms and Trojan horses being the major cyber threats. The focus was more towards malwares such as virus, worms and Trojans with purpose of causing damage to the systems. Cyber threats randomly targeted computers directly connected to the Internet. Artificial Intelligence methods are robust and more flexible; as a result expanding security execution and better defense system from an increasing number of advance cyber threats. Different AI techniques can be used in cyber security such as intelligent agent, neural nets, expert system, data mining, machine learning and deep learning.

4. Deep Learning Methods used in Cyber Security

This section describes the different DL methods used in cyber security. References to important methodology papers are provided for each technique. Machine learning is an effective tool that can be employed in many areas of information security. There exist some robust anti- phishing algorithms and network intrusion detection systems. Machine learning can be successfully used for developing authentication systems, evaluating the protocol implementation, assessing the security of human interaction proofs, smart meter data profiling, etc. Machine learning has presented a significant opportunity to the cyber security industry. New machine learning methods can vastly improve the accuracy of threat detection and enhance network visibility thanks to the greater amount of computational analysis they can handle. They are also heralding in a new era of autonomous response, where a machine system is sufficiently intelligent to understand how and when to fight back against in-progress threats. Different machine learning methods have been successfully deployed to address wide-ranging problems in computer security. We are to discuses three areas where most cyber ML algorithms are finding application: spam detection, malware analysis and intrusion detection.

4.1 Spam & Phishing Detection

Spam and phishing detection includes a large set of techniques aimed at reducing the waste of time and potential hazard caused by unwanted emails. Nowadays, unsolicited emails, namely phishing, represent the preferred way through which an attacker establishes a first foothold within an enterprise network. Phishing emails include malware or links to compromised websites. Spam and phishing detection is increasingly difficult because of the advanced evasion strategies used by attackers to bypass traditional filters. ML approaches can improve the spam detection process. Spam filtering based on the textual content of email messages can be seen as a special case of text categorization, with the categories being spam and nonspam. Today the most successful spam filters are based upon the statistical foundations of Machine Learning. Machine Learning based spam filters [Bla 08] also retrain themselves while put in use and minimizes manual effort while delivering superior filtering accuracy.

Although the task of text categorization has been researched extensively, its particular application to email data and detection of spam specifically is relatively recent. Some initial research studies primarily focused on the problem of filtering spam whereby Naïve Bayes (NB) was applied to address the problem of building a personal spam filter. Naive Bayes is a classic machine learning algorithm in which we can use all our feature to detect whether they become malicious file or not and used it for the purpose of classification. NB was advocated due to its previously demonstrated robustness in the textclassification domain and due to its ability to be easily implemented in a cost-sensitive decision framework. Although high performance levels were achieved using word features only, it was observed that by additionally incorporating non-textual features and some domain knowledge, the filtering performance could be improved significantly. Phishing is aimed at stealing personal sensitive information. Many Researchers have identified three principal groups of anti-phishing methods: detective (monitoring, content filtering, anti-spam), preventive (authentication, patch and change management), and corrective (site takedown, forensics) ones.

4.1.1 E-Mail Spam filterning

Automatic e-mail classification uses statistical approaches or machine learning techniques and aims at building a model or a classifier specifically for the task of filtering spam from a users mail stream. The building of the model or classifier requires a set of preclassified. The process of building the model is called training. Machine learning algorithms have achieved more success among all previous techniques employed in the task of spam filtering. In fact, the success stories of Gmail, can be ascribed to their timely transition and successful use of Machine Learning for filtering not just incoming spam but other abuses like Denial-ofService (DoS), virus delivery, and other imaginative attacks.

4.2 Malware Detection

Malware detection is an extremely relevant problem because modern malware can automatically generate novel variants with the same malicious effects but appearing as completely different executable files. These polymorphic and metamorphic features defeat traditional rule-based malware identification approaches. Malware can be divided into several classes depending on its purpose: virus, worm, Trojan, adware, spyware, root kit, backdoor, key logger, Ransom ware and Remote Administration Tools. ML techniques can be used to analyze malware variants and attributing them to the correct malware family.

4.3 Intrusion Detection

An Intrusion Detection System (IDS) is a defense measure that supervises activities of the computer network and reports the malicious activities to the network administrator. Intruders do many attempts to gain access to the network and try to harm the organization’s data. Thus the security is the most important aspect for any type of organization. Intrusion detection aims to discover illicit activities within a computer or a network through Intrusion Detection Systems (IDS). Network IDS are widely deployed in modern enterprise networks. These systems were traditionally based on patterns of known attacks, but modern deployments include other approaches for anomaly detection, threat detection and classification based on machine learning. Within the broader intrusion detection area, two specific problems are relevant to our analysis: the detection of botnets and of Domain Generation Algorithms (DGA). A botnet is a network of infected machines controlled by attackers and misused to conduct multiple illicit activities. Botnet detection aims to identify communications between infected machines within the monitored network and the external command- and-control servers. Despite many research proposals and commercial tools that address this threat, several botnets still exist. DGA automatically generate domain names, and are often used by an infected machine to communicate with external server(s) by periodically generating new hostnames. They represent a real threat for organizations because, through DGA which relies on language processing techniques, it is possible to evade defenses based on static blacklists of domain names.

Network Intrusion Detection (NID) systems are used to identify malicious network activity leading to confidentiality, integrity, or availability violation of the systems in a network. Many intrusion detection systems are specifically based on machine learning techniques due to their adaptability to new and unknown attacks.

Although machine learning facilitates keeping various systems safe, the machine learning classifiers themselves are vulnerable to malicious attacks. There has been some work directed to improving the effectiveness of machine learning algorithms and protecting them from diverse attacks.

Conclusion

While it is difficult to say which effects of machine learning – positive or negative – will prevail, what is an undeniable is the growing use of ML-powered systems on both sides of the cybersecurity divide, irreversibly transforming safety of the whole internet. Machine learning approaches are increasingly employed for multiple applications and are being adopted also for cyber security, hence it is important to evaluate when and which category of algorithms can achieve adequate results. We analyze these techniques for three relevant cyber security problems: intrusion detection, malware analysis and spam detection. Machine learning as a technology has erupted vastly in the whole cyber implementation space. These decision making algorithms are known to solve several problems. There are many opportunities in information security to apply machine learning to address various challenges in such complex domain. Spam detection, virus detection, and surveillance camera robbery detection are only some examples. Machine learning techniques have been applied in many areas of science due to their unique properties like adaptability, scalability, and potential to rapidly adjust to new and unknown challenges.

References

>>Kanal, E. (2017, January). Machine Learning in Cybersecurity. Carnegie Mellon University Software Engineering Institute. March 9, 2018

>>M. Chandrasekaran, K. Narayanan, and S. Upadhyaya, “Phishing Security Conference, 2006

>>A. Khan, B. Baharudin, L. H. Lee, and K. Khan, “A review of machine learning algorithms for textdocuments classification,” Journal of advances in information technology, 2010.

>>P. Torres, C. Catania, S. Garcia, and C. G. Garino, “An analysis of Recurrent Neural Networks for Botnet detection behavior,” in IEEE Biennial Congress of Argentina (ARGENCON), 2016.

>>M. I. Jordan and T. M. Mitchell, “Machine learning: Trends, perspectives, and prospects,” Science, 2015.

>> Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, 2015.

>> A. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, 2015.

>> E. Blanzieri and A. Bryl, “A survey of learning-based techniques of email spam filtering,” Artificial Intelligence Review, 2008.

>> J. Gardiner and S. Nagaraja, “On the Security of Machine Learning in Malware C8C Detection,” ACM Computing Surveys, 2016.