Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security

https://doi.org/10.3991/ijim.v14i16.16953

Mohammed I. Alghamdi (✉)
Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia
mialmushilah@bu.edu.sa

Abstract—The research aimed to conduct an extensive study of machine learning and deep learning methods in cybersecurity. To accomplish the objectives, the research carried out a qualitative study based on secondary data collection to review the available studies and literature. The research has examined three machine learning methods and three deep learning methods to study the most popular techniques used in cybersecurity. During the research, the working mechanism of each method was studied along with their strengths and weaknesses. Also, a comparative discussion has been made to examine the most effective method for cybersecurity. Limitations in the current literature were also identified, and future direction is also given to target and develop the weak areas of machine learning and deep learning methods.

Keywords—Machine learning, Deep learning, Cybersecurity, Applications

1 Introduction

The world has significantly changed after the third industrial revolution, and the emergence of industry 4.0 has been highly influential in changing the way businesses operate. The increasing use of machines and advanced technology created various problems for human beings like control and monitoring of the machines[1]. Therefore, humans began to automate the operations of businesses by using information technology. Gradually, the world began to observe a shift towards advanced technology, which digitized a significant portion of the processes and daily activities of the people. This major shift in the world paradigm caused the people to embrace new technologies that primarily based upon the use of data and information systems. The emergence of the internet and faster computers made the transition more rapid, and the world moved towards an automated and digitized format that caused advanced technologies to intrude into the lives of the people[2]. Currently, the human race is using technology for a large number of personal and professional activities, which mainly include communication and business operations. Therefore, with time, human activities were engulfed by the use of technology and advanced systems. Although these modern technologies solve a significant number of problems as they make human tasks easier and faster, they also bring with themselves a new set of advanced challenges and threats. These challenges mainly include the rise of the cybercrimes that are making businesses and people vulnerable to the data thefts, online frauds, loss of confidential information, etc.[3]. Therefore, the experts are working tirelessly to solve the problem of cybercrime by developing secure systems.

Cybercrimes emerged with the increasing use of internet and data systems that began to threaten the privacy of people and businesses. Therefore, to counter the emerging threats of cybercrime, experts began to work on cybersecurity, which developed into a new area of study with time. Cybersecurity is one of the essential requirements for all the businesses in the current era[4]. Therefore, cybersecurity experts have begun to apply machine learning and deep learning methods to design and implement secure systems. Deep learning and machine learning are advanced technologies that are in the emerging phase, which were initially used for automating the systems and machines. However, with time, the researchers observed their high potential and their applicability to multiple areas like cybersecurity. Therefore, cybersecurity practitioners began to study the effectiveness of deep learning and machine learning in cybersecurity. Hence, a large number of methods of deep learning and machine learning have been developed that are being used by cybersecurity professionals. However, these methods are still in the phase of the study, which has limited their large-scale use[5]. Also, these methods have their own threats and challenges, which need more research to make them highly efficient in implementing highly secure system protocols. Therefore, this research also aims to study different methods of deep learning and machine learning that are used in cybersecurity. This research performs an in-detail study of the mechanisms of deep learning and machine learning methods along with their strengths and weaknesses. The following sections contain a thorough discussion of the deep learning, machine learning, cybersecurity, methods used in cybersecurity, and future prospects of this area of study.

2 Methods and Material

The research is based on a qualitative approach that deals with the patterns and trends underlying in the research information. The qualitative research is highly beneficial in studying the targeted area with high flexibility and precision[6]. Therefore, research has used a qualitative approach to study the methods of machine learning and deep learning used in cybersecurity. Under this approach, the secondary data collection technique was used as this data collection method helps in studying the available studies and literature to examine the research area. Secondary data collection helps in identifying the existing strengths and weaknesses of the research topic[7]. Therefore, this study examines the strengths and weaknesses of the learning method to provide insight for future research. Under this data collection method, pertinent journal articles, textbooks, and credible web articles were accessed to extract relevant information. To ensure the inclusion of updated information, researches published from 2013-2020 were considered. Additionally, to extract most relevant researches, particular keywords were used, i.e., survey of machine learning and deep learning methods, machine learning and deep learning methods in cybersecurity, machine learning and deep learning techniques. To further refine the searches, Boolean operators were also used, like “deep learning” AND “machine learning” AND “cybersecurity”.

3 Machine Learning

Machine learning is the branch of artificial intelligence that works to provides machines and systems to learn automatically from experience without the need for explicit programming. According to Jordan and Mitchell[8], machine learning algorithms help the systems use the data collected while the operation to learn and develop new abilities. For instance, the machines can learn to turn themselves off in case of any emergency. Therefore, machine learning algorithms are highly beneficial in improving the performance of the systems. Machine learning has an extensive application that ranges from computer systems to large industrial machines, which can be automated with the help of machine learning programs. In addition to this, machine learning algorithms are being used increasingly for developing self-learning programs that can provide multiple benefits to businesses[9]. Programs like smart business analytics are an example of machine learning that are enabling businesses to improve their decision-making power and improve their efficiency. Furthermore, the machine learning methods are being used for developing cybersecurity systems that can keep the data storage and processing safe for the businesses.

These machine learning programs help the businesses design and implement a high-quality security system that can learn from the security data fed into it. Machine learning methods can study the patterns in the data and get trained to prevent similar cyber-attacks in future[5]. Also, they help the businesses to be prepared for the changing pattern of the cyber-attacks by self-improving themselves, without the need for external programming. Therefore, cybersecurity systems that are based on machine learning codes, seldom require updates and maintenance as they can keep themselves up to date via learning from the collected data. However, these systems largely depend on the data, which can cause the problem of biasness in their actions[8]. Hence, it is imperative that high-quality data should be fed into these systems so that the machine learning methods can work accurately to provide high cybersecurity.

4 Shallow and Deep Learning

Machine learning can be divided into two primary branches, shallow learning and deep learning. Shallow learning was the initially used methods of learning that based on the learning of data without using networking or relational details of the data[10]. Therefore, the lack of links between the old and new data causes shallow learning programs to learn irrelevant details that can harm the systems or increase its size unnecessarily. However, the shallow learning methods are faster as compared to the deep learning methods, which is the primary reason they are continually used in the cybersecurity systems. Also, shallow learning methods are referred to as the conventional machine learning methods as they require human input during the structuring of data. This feature of machine learning causes the cybersecurity specialists to define the behavior of the systems based as per their requirements[9]. Thus, machine learning methods prove to be highly effective in various areas of cybersecurity.

On the other hand, deep learning methods are an advanced version of machine learning methods. Deep learning, as the name defines, is an in-detail method of learning that ensures only relevant information is extracted and used for system development and improvement. This practice of learning is brought about by the linking of the old data with the new data to identify the patterns and validate the accuracy of the data[11]. Network layers are one of the most important features of the deep learning method that helps in the efficient learning process. However, one of the major limitations of these methods is that they are time-consuming as they include various process before learning is performed. Also, these methods are more complex than the shallow machine learning methods and thus, require more carefulness and expertise of the developers. Nevertheless, deep learning methods provide an automated learning process that requires minimal human input; once they are operational, they reduce the maintenance requirements[12, 13]. Therefore, deep learning methods are also applied to the cybersecurity systems as they can provide an effective and timely response to cyber threats.

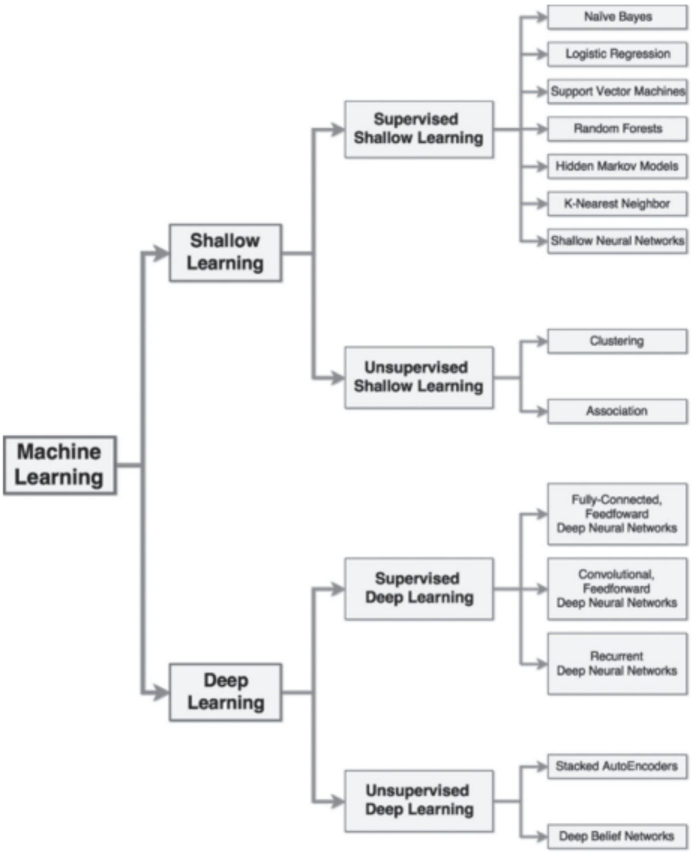

Fig. 1. Classification of machine learning[11]

5 Cyber Security

Cybersecurity is one of the most important areas of study and practice for IT experts. According to Jang-Jaccard[4], cybersecurity is defined as the procedures and policies adopted to protect the computers, databases, servers, and networks from the cyber threats like attacks, thefts, malware, etc. The increasing digitization of the process all over the world has made the cybercriminals highly active, who are working to intrude into the confidential information of the people and organizations to gain financial and personal benefits. Therefore, the threats to the information systems are severe, which need to be given high protection so that any malicious attack can be prevented[14]. Hence, cybersecurity practitioners are also working to continuously evolve the security systems and standards that can keep the people and organizations safe from loss of data or capital. Cybercrimes are also being used by the competitors of the organizations to steal the intellectual property and inflict harm to their businesses so that the formers can gain a leading position in the market. Therefore, all the organizations are working to ensure that they have the highest quality cybersecurity system that can keep their systems and data safe.

Cybersecurity can be classified into the following categories, based on their area of working[15]:

- Network security: This type of cybersecurity systems are keeping the networks and communication of the organizations safe from the intruders.
- Application security: This cybersecurity protocol ensures that the applications and software are safe from any malicious activity that can cause loss of data.
- End-user security: This practice keeps the users of the system educated so that they can work safely and avoid any cyber threats.
- Operational security: Business operations usually require handling and transporting a large quantity of data. Its safety is highly important to keep the organizations running, which is ensured by cybersecurity.
- Informational security: This type of security keeps the databases safe from intruders and hackers, who may want to access the information for their personal or financial gains.
- Disaster recovery and business continuity: This practice of cybersecurity is a response to the cybersecurity incident, which may have caused a loss of data. Thus, these methods ensure that all the lost data is recovered and operations are back to normal.

Machine learning and deep learning methods can perform all of the stated functions of cybersecurity, which makes them highly effective in protecting the systems and data[16]. These advanced methods are being used in the cybersecurity to keep the data, systems, users, and organizations safe from malicious attacks. Also, their high accuracy and efficiency along with the ability to improve themselves automatically have made machine learning and deep learning methods highly effective in the area of cybersecurity.

6 Methods of Machine Learning and Deep Learning Used in Cyber Security

6.1 Decision Trees

Decision Trees are one of the oldest methods of machine learning. This method has been used for several problem-solving applications like automation of machines, decision-making in robots, cybersecurity, etc. Classification is the main strength of this method of machine learning, as it uses a tree format to structure the data and properties logically[17]. The classification of the properties helps the program to make predictions by using structured data. This method is highly efficient in cybersecurity as it uses the tree that is based on nodes, which represents the properties and each leaf represent a category. Therefore, by using multiple properties and categories, it structures the collected data and analyzes it according to the types and severity of the cyber threat. A decision tree is a machine learning method used to develop predictive models. This method is used to map object attributes and object values[18]. In addition, nodes also represent the value of the object that can be derived from the root node to the leaf node. ID3, C4.5 and CART are the most commonly used decision trees (figure 2 shows an example of a decision tree).

Decision trees can be applied to various domains of cybersecurity like intrusion-detection and determining the paths of a potential attack. However, its major use has been in the detection of possible intrusions[19]. The experts are using the existing data of intrusions made in the past to design and train the decision trees so that they can make the system prune to the possible intrusion in future. However, this method of machine learning has a major limitation that it cannot be used against the unknown ways of intrusion. The cybercriminals are becoming advanced with time and are employing new ways to intrude into the systems[20]. Therefore, this method requires frequent updates and training of the model to keep it effective against the advanced techniques of cyber-attacks. Hence, this limitation of this method has urged the expert to research and develop advanced methods of cybersecurity.

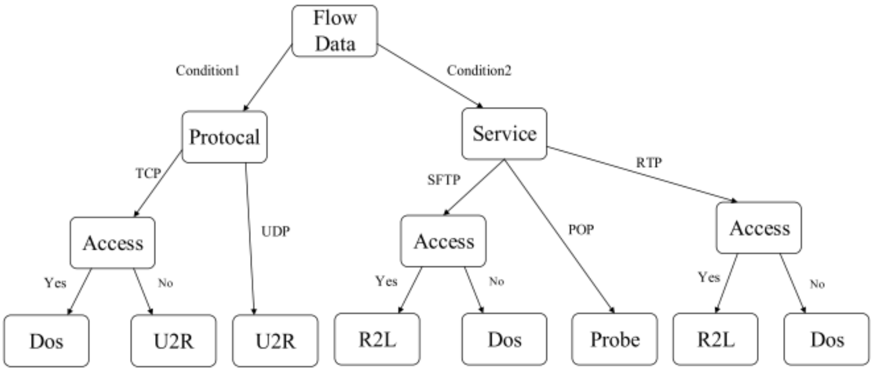

Fig. 2. A typical decision tree[17]

6.2 Support Vector Machine

Support Vector Machine (SVM) is another machine learning method that is applied to the cybersecurity[21]. Unlike the decision trees, this method uses the boundary concept to separate the set of instances that have different class values. SVC can work on single to multi-class types depending on the types of data used to train the model. The model classifies the data by separating the input vectors from the positions via separation hyperplane, each of them lying on either side of the hyperplane. SVM uses kernel functions to map and classify the data points that are not linear[22]. This model is mainly based on the use of vectors and distances that define the properties and values of the data used to train the SVM model. Therefore, this method is less complex than the decision tree methods as it can be trained by developing an equation that applies to various conditions.

SVM is mainly used for intrusion detection in the area of cybersecurity. The method of intrusion detection using SVM can be classified into four stages. Data pre-processing is the first stage that involves the converting of the raw data into useful data by refining it to ensure that irrelevant data is removed. The next step involves the conversion of data to LibSVM format that includes the procedures of training and testing data to convert it to numerical values[23]. Also, classes of the dataset are determined based on their values to be used during the classification stage. The third stage is the optimization of the data using SVM and PSO. The NSL-KDD dataset in LibSVM format is scaled in[24]. The scaling process reduces the impact of the outliers on the data values, ensuring higher accuracy of the model. Thus, this method improves the performance of the SVM model. The last and fourth stage of the process involves the classification of data using SVM. The system is trained by using SVM and dataset to classify it according to the target value and several attributes. This process aims to develop a model that has the ability to predict the potential threat of intrusion by using target values and attributes of data used to train the model[25]. Thus, this method is also dependent on the human programmers to structure and train the model as this method cannot refine the data by itself. Hence, this is a major limitation of this method.

6.3 K-Nearest Neighbor

K-Nearest Neighbor (KNN) is a machine learning method used in various systems, including cybersecurity[17]. This method calculates the distance between two instances, which is used to develop the model, by using the following formula:

$$d(x, y) = \sqrt{\sum_{k=1}^{n}(x_k - y_k)^2}$$

Fig. 3. Equation for KNN[17]

Where, x_k and y_k are the kth featured element of instance x and y respectively. Whereas, n is the total number of features in the dataset. The algorithm of KNN work by calculating the distances between the two elements of the instances in the dataset. These distances are used by the model to identify the patterns in the data that is used to train them. The data fed into these models is primarily of the normal working behavior of the people and possible behavior of the intruders[26]. This data helps the KNN model to determine the normal working patterns, by using which it stops any possible intrusion into the system. However, this method also has a disadvantage that its use cannot stop the novel intrusion methods[27]. Also, this method requires the calculation of the distances of the elements in the instances of the dataset. A dataset has a large number of classes, which have various instances. Thus, this is a complex method to develop and train a machine learning model.

Nevertheless, the use of a general formula and no requirement of building a separate profile for different programs make this method convenient to be used for cybersecurity. In addition to this, this method uses the calculation of the distance of two elements at one time, which makes it easier to identify the anomaly in the data sets[28, 29]. These anomalies are usually referred to as the unusual working behavior, which can be attributed the intruders. Therefore, highly accurate detection of anomalies makes this method very effective in intrusion detection. Hence, this method can be used to design and develop secure IT systems to be used in organizations.

6.4 Deep Belief Networks

Deep Belief Network (DBNs) are one of the commonly used deep learning methods. This method of learning is based on the use of a network that has various layers of hidden units with relations between them[30]. This method of deep learning is an unsupervised training technique that is highly effective in cybersecurity. The minimal requirement of human interaction with DBNs has been mainly attributed to the ability of the system to enhance and improve itself. Therefore, by self-learning, DBNs can prune the systems against novel and advanced threats of cybersecurity. DBNs are trained systematically, in which each of the layers is trained individually to make highly effective training of the model that can identify the patterns and predict the future conditions[17]. DBNS are mainly used for the detection of intrusions and malware into the systems. These two are the most common cyber threats that exist in the world, and DBNs have been observed to be highly effective in these areas[31-33]. Therefore, the use of DBNs is increasing to train cybersecurity models that can provide high security to the organization's data and systems.

Moreover, the training method of DBNs is highly efficient as it trains one layer at a time, which reduce the use of computational resources to build highly effective models. The performance of the DBNs has been tested by several researchers, who state that the detection rate of DBN models is about 99% when NSL-KDD data is used[34]. Also, the models are highly accurate, with about 98% accuracy to correctly identify the false data injection. However, it has also been studied that the unsupervised training of DBN models is also a threat to their effectiveness and accuracy as they can develop biasness with time. Continuous learning based on similar data can make them effective against limited cyber threats, while ineffective against the others[35]. Therefore, the experts are studying this area of the DBN model and have developed the use of increased layers that does not allow the model to become biased. Therefore, through an intensive training process, these models are highly effective against most of the cyber threats.

6.5 Recurrent Neural Networks

Neural networks are one of the basic methods of deep learning, which are trained in a supervised manner. Recurrent neural network (RNN) is an advanced type of neural networks, which does not have limited abilities like traditional neural networks[17]. The traditional neural network has a limitation that they can only take fixed-length data inputs, which makes their ability to handle input sequences of variable lengths, less effective. RNN has an advantage in this area as the output of the hidden units is used as extra input for the next element, and processes inputs, one at a time. Thus, the RNNs are highly effective in handling the problems of speech and language, along with time series problems. On the other hand, RNNs have a drawback due to their challenging process of training the model[34]. The complex arrangement of layers and elements is the major reason for a difficult training process, which is making the experts study the area more extensively. Therefore, the advanced study in the training process and architecture of the RNN model is significantly improving the efficiency of the RNN models.

RNN model is being used in several domains of cybersecurity like traffic analysis, malware, and intrusion detection. This method of deep learning uses the technique of random temporal projection to extracting full information from the data and use it to secure the systems against malware and intrusion[36]. RNNs also analyses the patterns of the data by communicating between multiple layers and elements at a time to reach an accurate result. Thus, by carrying out an extensive analysis and learning of data, RNNs gain the ability to fight against various cyber threat. Also, they have a feature of predicting the patterns for the future, which also makes them effective against unknown ways of intrusion. The experts also have advanced RNNs by using long-short memory method (LSTM), which makes these models learn the data from the smallest to a very large range[37]. Thus, LSTM enables RNNs to develop very long memory, which makes analysis of data and identification of patterns and relations more accurate. LSTM units comprise of a structure called a memory cell that gathers information. These memory cells act like a human brain comprising of the ability to identify potential threats, learn from experiences, and act against the threats. Moreover, RNN also has another memory unit that provides it with a long memory, which is the gated recurrent unit (GRU)[38]. GRUs work in a similar manner as the LSTM units; however, they are less complex as they have fewer parameters, making their training process easier. Therefore, the use of RNN model for cybersecurity is one of the most effective methods due to its ability to address the majority of the cybersecurity problems.

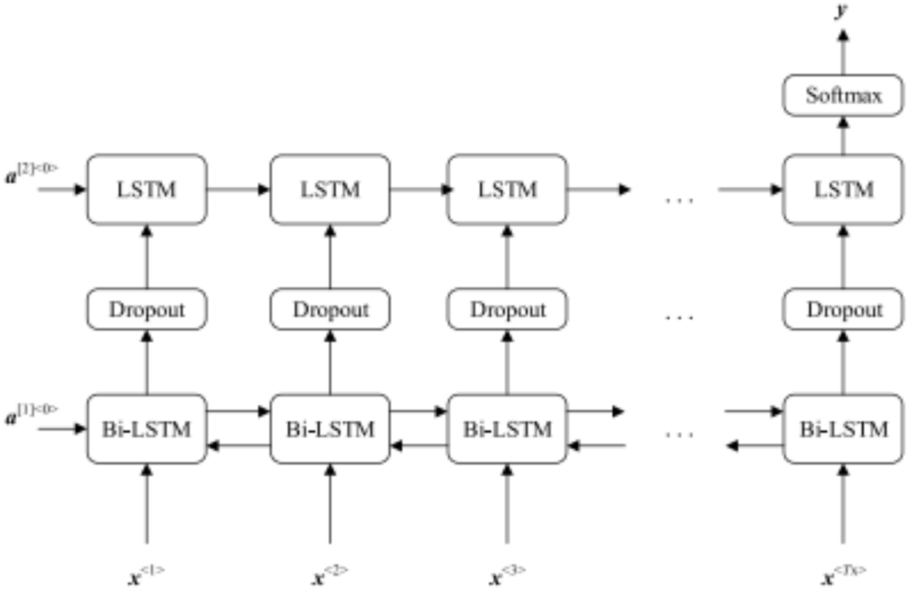

Fig. 4. A typical RNN structure[17]

6.6 Convolutional Neural Networks

Convolutional neural networks (CNNs) are another type of neural networks, based on deep learning method. This method structures the data in the form of arrays. These arrays enable the classification of the data systematically separating the classes according to their properties. In addition to this, the use of arrays also provides CNNs with the ease of presenting the results as 2D pixels[34]. CNNs are often employed to process the 2D arrays of images or spectrograms of audio. Also, they are applicable for 3D arrays like videos and volumetric images. CNNs are highly effective in structuring the data based on their spatial and temporal properties. Thus, making the process of learning easier. Moreover, CNNs have three distinct layers that make up the learning model, which include pooling layers, convolution layers, and the classification layer[17]. Convolution layer is the fundamental part of the CNN model, which are defined by the weights of the original input of the data. The results of the convolution layer are passed through a feature map to develop physical or temporal relationships within the data[39]. These practices have an advantage that a long memory can be stored by using small space and developing an extensive network of the data.

Furthermore, the pooling layers perform non-linear down sampling by applying a specific function. These layers reduce the size of the feature maps allowing a large memory to be stored in a small space[40]. This enhances the learning ability of the model. CNNs are most commonly trained by using the technique of “dropout”, which enables the model to perform iterations, which removes the irrelevant information from the layers, making the model highly effective for the cybersecurity applications. Dropout also enhances the accuracy and generalizability of models, making them highly efficient at identifying unusual behavior[41]. Also, these models are self-learning models that learn from the experiences and patterns available in the data, which makes them highly effective against malware and intrusion. However, this method of deep learning is complex and time-consuming, which limits its use in some of the cybersecurity systems[42]. Nevertheless, with continued research of the experts, it is anticipated that these methods will become more popular in future as the complexity of the training process will reduce with time.

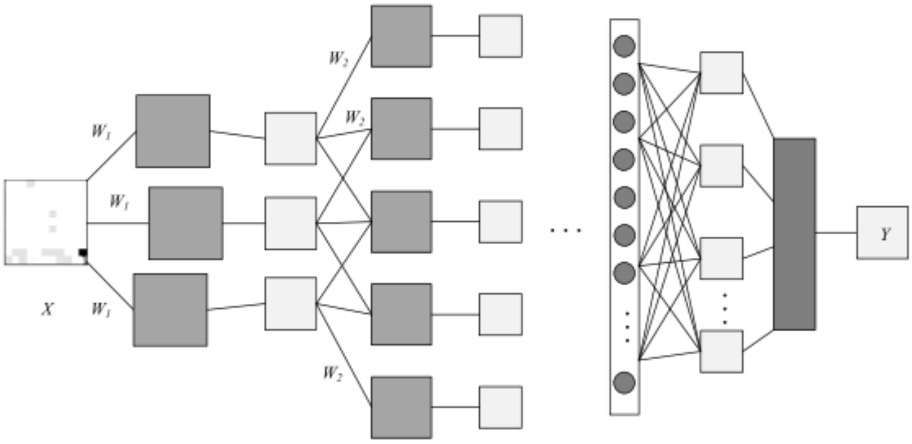

Fig. 5. An example of CNN[17]

7 Discussion and Future Direction

The above research has discussed and examined three machine learning methods and three deep learning methods that can be used in cybersecurity systems. The analysis has found a major observation that the machine learning method offers a shallow learning process, which makes them less effective in handling the cybersecurity threats as compared to the deep learning methods[39, 43]. Decision trees are the most widely used method of machine learning that helps the cybersecurity personnel to employ a security system that can solve the cybersecurity problems. However, these models are dependent on humans to structure the data and are ineffective against novel threats[17, 44]. In addition to this, KNN and SVM methods are also dependent on the human force to structure the data, but they are less complex than the decision trees. Nevertheless, KNN and SVM methods use a complex training process, which makes them less effective in handling all the problems of cybersecurity. Therefore, it can be stated based on the analysis that the machine learning methods have some limitations that are making their use in cybersecurity less popular.

The experts have moved towards more advanced methods of machine learning, i.e. deep learning, to overcome the limitations of shallow learning. This research has examined DBN, RNN, and CNN methods of deep learning that are being studied and applied to the cybersecurity systems. DBN methods are popular among the experts due to the unsupervised training of the model as compared to RNN and CNN that need supervised training[31]. Also, the training process of DBN is more efficient as they train one layer at a time, giving out highly accurate results. On the other hand, RNN and CNN are more complex at training due to their structure and requirement of human input. However, RNN and CNN offer a highly extensive structure that is based on multiple links of the instances and classes of the data, which makes the identification of the pattern highly accurate. Also, these methods have an increased ability to store long memory, which enhances their prediction abilities[40]. Among RNN and CNN, it has been observed that CNN is more challenging to train the models; however, it offers the highest accuracy of intrusion detection and prevention of cyberattacks. Therefore, it can be stated that CNN is the most effective method of deep learning that can be used for cybersecurity systems.

However, there are some limitations in each of the methods that can be improved with further research in future. The most critical areas that require more research to enhance the abilities of the learning methods are training procedures, structuring and refining of data, improving action against novel cyber threats[11, 17, 45, 46]. Training procedures need to be further researched and improved so that the models can be trained with ease using less time and resources. Additionally, the structuring and refining of data is a complex process that directly affects the efficiency of the models to provide cybersecurity. Therefore, by more research and development in this area, high-quality data can be used for training the models. Similarly, the methods of deep learning and machine learning have certain limitations to fight the novel cybersecurity threats. Hence, more study is required to provide the models with an enhanced ability to protect against the advanced and novel cybersecurity threats.

8 Conclusion

In the end, it can be concluded that machine learning and deep learning methods have a high potential to address and solve the cybersecurity problems. The advanced threats of cybersecurity posed to the organizations and individuals can be solved with high efficiency by using machine learning and deep learning methods. The machine learning methods like decision trees, SVM, and KNN are most common and are being further studied to enhance their effectiveness in solving the problems of cybersecurity. However, deep learning methods like DBN, RNN, and CNN are more advanced than machine learning methods. Also, they offer high effectiveness in fighting cybersecurity threats like intrusion, malware, and theft. Nevertheless, these methods still have some limitation like complex training procedure, inefficiencies in fighting novel threats, and complex structure of data. Therefore, more research is needed in these areas to enhance further, the efficiencies of the machines learning and deep learning methods in cybersecurity.

9 References

[1] M. Yar and K. F. Steinmetz, *Cybercrime and society*. SAGE Publications Limited, 2019.

[2] E. R. Leukfeldt, "Cybercrime and social ties," *Trends in organized crime,* vol. 4, no. 17, pp. 231-249, 2014.

[3] E. R. Leukfeldt and M. Yar, "Applying routine activity theory to cybercrime: A theoretical and empirical analysis," *Deviant Behavior,* vol. 3, no. 37, pp. 263-280., 2016. https://doi.org/10.1080/01639625.2015.1012409

[4] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences,* vol. 5, no. 80, pp. 973-993, 2014. https://doi.org/10.1016/j.jcss.2014.02.005

[5] S. Dua and X. Du, *Data mining and machine learning in cybersecurity*. CRC press, 2016.

[6] E. Hildt, K. Lieb, and A. G. Franke, "Life context of pharmacological academic performance enhancement among university students–a qualitative approach," *BMC medical ethics,* vol. 1, no. 15, pp. 1-10., 2014. https://doi.org/10.1186/1472-6939-15-23

[7] M. P. Johnston, "Secondary data analysis: A method of which the time has come," *Qualitative and quantitative methods in libraries,* vol. 3, no. 3, pp. 619-626, 2017.

[8] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science,* vol. 349, no. 6245, pp. 255-260, 2015. https://doi.org/10.1126/science.aaa8415

[9] E. Brynjolfsson and A. Mcafee, "The business of artificial intelligence," *Harvard Business Review,* pp. 1-20, 2017.

[10] C. Zhang and Y. Ma, *Ensemble machine learning: methods and applications*. Springer Science & Business Media, 2012.

[11] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *2018 10th International Conference on Cyber Conflict (CyCon)*, 2018. https://doi.org/10.23919/cycon.2018.8405026

[12] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.

[13] O. H. Yahya, H. Alrikabi, I. A. J. I. J. o. O. Aljazaery, and B. Engineering, "Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network," vol. 16, no. 03, pp. 107-116, 2020. https://doi.org/10.3991/ijoe.v16i03.13021

[14] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Computers in Human Behavior,* vol. 48, pp. 51-61, 2015. https://doi.org/10.1016/j.chb.2015.01.039

[15] M. Akbari Roumani, C. C. Fung, S. Rai, and H. Xie, "Value analysis of cyber security based on attack types," *ITMSOC: Transactions on Innovation and Business Engineering,* vol. 1, pp. 34-39, 2016.

[16] J. B. Fraley and J. Cannady, "The promise of machine learning in cybersecurity," in *SoutheastCon 2017*, 2017. https://doi.org/10.1109/secon.2017.7925283

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

[18] U. Adhikari, T. Morris, and S. Pan, "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Transactions on Smart Grid,* vol. 8, no. 6, pp. 2744-2753, 2016. https://doi.org/10.1109/tsg.2016.2537210

[19] J. M. Torres, C. I. Comesaña, and P. J. García-Nieto, "Machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics,* vol. 10, no. 10, pp. 2823-2836, 2019. https://doi.org/10.1007/s13042-018-00906-1

[20] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," *Computer Science Review,* vol. 29, pp. 44-55, 2018. https://doi.org/10.1016/j.cosrev.2018.05.003

[21] K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan, and J. A. Chambers, "Support Vector Machine for Network Intrusion and Cyber-Attack Detection," in *2017 Sensor Signal Processing for Defence Conference (SSPD)*, 2017. https://doi.org/10.1109/sspd.2017.8233268

[22] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," in *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

[23] A. Abdiansah and R. Wardoyo, "Time complexity analysis of support vector machines (SVM) in LibSVM," *International journal computer and application,* vol. 128, no. 3, pp. 28-34, 2015. https://doi.org/10.5120/ijca2015906480

[24] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications surveys & tutorials,* vol. 18, no. 2, pp. 1153-1176, 2015. https://doi.org/10.1109/comst.2015.2494502

[25] M. A. Hashmani, S. M. Jameel, A. M. Ibrahim, M. Zaffar, and K. Raza, "An Ensemble approach to Big Data Security (Cyber Security)," *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS,* vol. 9, no. 9, pp. 75-77, 2018. https://doi.org/10.14569/ijacsa.2018.090910

[26] D. A. Adeniyi, Z. Wei, and Y. Yongquan, "Automated web usage data mining and recommendation system using K-Nearest Neighbor (KNN) classification method," *Applied Computing and Informatics,* vol. 1, no. 12, pp. 90-108, 2016. https://doi.org/10.1016/j.aci.2014.10.001

[27] A. I. Abubakar, H. Chiroma, S. A. Muaz, and L. B. Ila, "A Review of the Advances in Cyber Security Benchmark Datasets for Evaluating Data-Driven Based Intrusion Detection Systems," *SCSE,* pp. 221-227, 2015. https://doi.org/10.1016/j.procs.2015.08.443

[28] M. Laštovička, A. Dufka, and J. Komárková, "Machine learning fingerprinting methods in cyber security domain: Which one to use?," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2018. https://doi.org/10.1109/iwcmc.2018.8450406

[29] I. A. Aljazaery, H. T. S. Alrikabi, and M. R. J. i. Aziz, "Combination of Hiding and Encryption for Data Security," vol. 14, no. 9, p. 35, 2020.

[30] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one,* vol. 11, no. 6, 2016. https://doi.org/10.1371/journal.pone.0155781

[31] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications,* vol. 50, no. 102419, 2020. https://doi.org/10.1016/j.jisa.2019.102419

[32] N. Hussien, I. Ajlan, M. M. Firdhous, and H. Alrikabi, "Smart Shopping System with RFID Technology Based on Internet of Things," 2020. https://doi.org/10.3991/ijim.v14i04.13511

[33] A. Alaidi, O. Yahya, and H. Alrikabi, "Using Modern Education Technique in Wasit University," 2020.

[34] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information,* vol. 10, no. 4, p. 122, 2019. https://doi.org/10.3390/info10040122

[35] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy internet," *Energy,* vol. 174, pp. 1292-1304, 2019. https://doi.org/10.1016/j.energy.2019.03.009

[36] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *2016 International Conference on Platform Technology and Service (PlatCon)*, 2016.

[37] H. Gasmi, A. Bouras, and J. Laval, "LSTM recurrent neural networks for cybersecurity named entity recognition," *ICSEA,* p. 11, 2018.

[38] L. Mou, P. Ghamisi, and X. X. Zhu, "Deep recurrent neural networks for hyperspectral image classification," *IEEE Transactions on Geoscience and Remote Sensing,* vol. 7, no. 55, pp. 3639-3655, 2017. https://doi.org/10.1109/tgrs.2016.2636241

[39] F. Ullah *et al.*, "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access,* vol. 7, pp. 124379-124389, 2019. https://doi.org/10.1109/access.2019.2937347

[40] H. Wu and X. Gu, "Towards dropout training for convolutional neural networks," *Neural Networks,* vol. 71, pp. 1-10, 2015. https://doi.org/10.1016/j.neunet.2015.07.007

[41] Y. D. Zhang, C. Pan, J. Sun, and C. Tang, "Multiple sclerosis identification by convolutional neural network with dropout and parametric ReLU," *Journal of computational science,* vol. 28, pp. 1-10, 2018. https://doi.org/10.1016/j.jocs.2018.07.003

[42] R. A. Demidov, P. D. Zegzhda, and M. O. Kalinin, "Threat analysis of cyber security in wireless adhoc networks using hybrid neural network model," *Automatic Control and Computer Sciences,* vol. 52, no. 8, pp. 971-976, 2018. https://doi.org/10.3103/s0146411618080084

[43] H. T. S. ALRikabi, A. H. M. Alaidi, and F. T. J. J. o. A. R. i. D. C. S. Abed, "Attendance System Design And Implementation Based On Radio Frequency Identification (RFID) And Arduino," p. 6.

[44] N. S. Alseelawi, E. K. Adnan, H. T. Hazim, H. Alrikabi, and K. Nasser, "Design and Implementation of an E-learning Platform Using N-Tier Architecture," 2020. https://doi.org/10.3991/ijim.v14i06.14005

[45] S. Abt and H. Baier, "A plea for utilising synthetic data when performing machine learning based cyber-security experiments," in *Proceedings of the 2014 Workshop on Artificial Intelligent and Security Workshop*, 2014. https://doi.org/10.1145/2666652.2666663

[46] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019. https://doi.org/10.1109/ccwc.2019.8666588

10 Author

Mohammed I. Alghamdi received the BS degree in computer science from King Saud University, Riyadh, Saudi Arabia, in 1999, the MS degree in computer science from Colorado Technical University, Denver, Colorado, in 2003, and the PhD degree in computer science from New Mexico Institute of Mining and Technology in 2008. Currently, he is an assistant professor with the Department of Computer Science, Al-Baha University, Kingdom of Saudi Arabia. His research interests include wireless networks, storage systems, parallel and distributed systems, computer system security, cluster. He is a senior member of the IEEE. His field interests are Cyber Security, Networks and Wireless Networks. Number of articles in international database: 34

Article submitted 2020-07-10. Resubmitted 2020-07-28. Final acceptance 2020-07-29. Final version published as submitted by the authors.