Computer Science Review 39 (2021) 100317

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review

Priyanka Dixit *, Sanjay Silakari

Department of Computer Science & Engg, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal (M.P), India

ARTICLE INFO

Article history:
Received 23 May 2020
Accepted 6 November 2020
Available online xxxx

Keywords:
Cybersecurity
Deep learning
Attack
Supervised and unsupervised

ABSTRACT

Cybersecurity mainly prevents the hardware, software, and data present in the system that has an active internet connection from external attacks. Organizations mainly deploy cybersecurity for their databases and systems to prevent it from unauthorized access. Different forms of attacks like phishing, spear-phishing, a drive-by attack, a password attack, denial of service, etc. are responsible for these security problems In this survey, we analyzed and reviewed the usage of deep learning algorithms for Cybersecurity applications. Deep learning which is also known as Deep Neural Networks includes machine learning techniques that enable the network to learn from unsupervised data and solve complex problems. Here, 80 papers from 2014 to 2019 have been used and successfully analyzed. 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. Each specific technique is effectively discussed with its algorithms, platforms, dataset, and potential benefits. The paper related to deep learning with cybersecurity is mainly published in the year 2018 in a large number and 18% of published articles originate from the UK. In addition, the papers are selected from a variety of journals, and 30% of papers used are from the Elsevier journal. From the experimental analysis, it is clear that the deep learning model improved the accuracy, scalability, reliability, and performance of the cybersecurity applications when applied in realtime.

Contents

* Corresponding author.
E-mail addresses: dixitpriyanka384@gmail.com, priyankadxt048@gmail.com (P. Dixit), ssilakari@yahoo.com (S. Silakari).

https://doi.org/10.1016/j.cosrev.2020.100317
1574-0137/

1. Introduction

Nowadays, cyberspace development is increasing rapidly because of cloud computing [1], big data [2], Internet of Things, and software-based network growth. One of the common problems in cyberspace is cybersecurity. Cybersecurity is a means of safeguarding the systems, applications, and networks from potential digital attacks. The main aim of the adversaries which conducts these attacks is to modify/access the confidential information, laundering money from the users, and interrupting the normal business operations. The challenges associated with implementing the cybersecurity policies on organizations are the large number of devices connected to the network and the novel attacks conducted by hackers. The different kinds of attacks are prevented by using tools like the intrusion detection system, firewalls, scanner, and antivirus software, etc. The devices connected to the network are often subjected to various attacks. The internet offers interconnection between networks as well as supports hardware, intelligence, software, information, and data to be exchanged between each other. Hence, computer networks are very vulnerable to malware or other cybersecurity attacks.

The attackers are experienced to trace out the data from cyberspace [3]. The huge volume of data and confidential information is shielded with cybersecurity and if any attacks happen they automatically alert the whole organization about the same. Moreover, the anomalous detection characteristics, event correlation, and pattern identification are classified using data science concepts applied to cybersecurity. The mobile devices cannot be protected by the Intrusion Detection System(IDS) because of the limited battery power, mobility, and energy consumption characteristics. A protective shield can be built to safeguard the applications using cybersecurity with the help of machine learning algorithms [4–8]. The modern computer system adds additional computational complexity when processing a huge amount of information and while offering security.

This challenge can be overcome by incorporating techniques of Artificial Intelligence(AI) [9]. The rapid development of computer-based research, methods, and applications to replicate human intelligence is called artificial intelligence (AI). The AI techniques can easily identify the malware present in the application and can take robust actions. It is also used to process the vast amount of information the users generate on a daily basis. Machine learning (ML) with more amounts of security detection software, encoding, and thread extraction characteristics are required to identify these attacks [10]. But, the deep learning concept is more efficient to detect the cybersecurity issues. Deep learning is one of the powerful machine learning techniques powered by AI and this research focuses on the same. The deep learning techniques can process a vast amount of information present in the cybersecurity datasets efficiently by withstanding the attacks [11]. Hence, many of the researchers focused on cybersecurity issues with deep learning concepts [12].

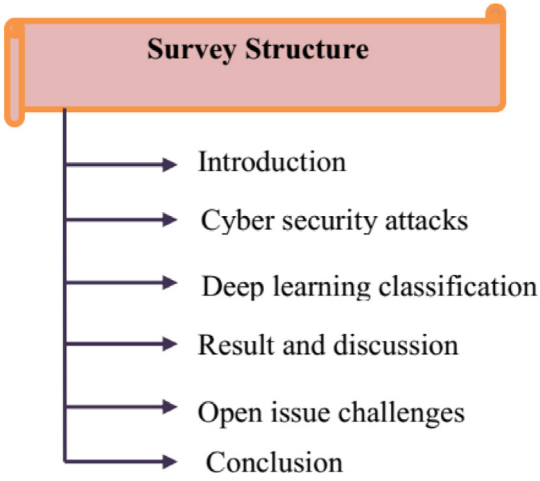

Fig. 1. Structure of cybersecurity attack detection survey.

These researchers [13–20] proposed an elaborate survey of existing cybersecurity applications utilizing deep learning techniques. These researches were mainly conducted to motivate various researchers pursuing their research in the same field to upgrade the security of different organizations vulnerable to various potential attacks. However, these articles did not cover the broad area of cybersecurity datasets used and the weaknesses present in these deep learning techniques. Therefore, the basic objective of this work is to introduce a bibliometric analysis of the deep learning approach used for the detection of potential threats to cybersecurity. Effectively, we have chosen the research papers from the year 2011 to 2020, which are based on cybersecurity issues with deep learning concepts. Ultimately, we analyzed 80 research papers from different kinds of journals and the deeply analyzed survey are effectively mentioned in the below section. Therefore, the outline structure of deep learning based on cybersecurity attack detection is described in Fig. 1.

The contribution of this review article is explained as follows:

i. We identify the different cybersecurity attacks namely denial of service, probe, malware, zero-day, phishing, sinkhole, and user root attacks, and how deep learning models solve these attacks.
ii. Next, the different variants of deep neural network models are analyzed and their functionalities are specified. The different types of neural networks studied are Convolutional Neural Network, Autoencoder, Deep Belief Network, Recurrent Neural Network, Generative Adversal Network, and Deep Reinforcement Learning.
iii. A comparative analysis is conducted to review the different attacks encountered, the diverse platform used, datasets, and learning models of various researchers in the field of cybersecurity using Deep Learning.
iv. This survey also provides the challenges faced by existing research and open issues

The rest of this paper is organized as: The cybersecurity attacks are formulated in Section 2. In Section 3, the deep learning-based cybersecurity attacks are discussed. Moreover, the current trend discussion and analysis are carried out in Section 4 as well as the challengeable open issues, and future research directions are formulated in Section 5. At last, the paper is summarized in Section 6.

2. Cybersecurity attacks

The cybersecurity system is affected by different kinds of attacks such as a denial of service, probe, malware, zero-day, phishing, sinkhole, user root, adversarial attacks, poisoning attack, evasive attack, Integrity attack, and causative attack. Most of the researchers have used deep learning concepts for the detection of these attacks. In this survey, we analyzed different papers related to cybersecurity attack detection with the help of deep learning concept and few of the attacks are discussed below. It also addresses the type of attackers and their goals.

2.1. Type of attackers

The attacker's knowledge can be classified into three types. In the black box attack, the attacker does not know anything about the deep learning model and they have zero knowledge about the model. In the gray box model, the attackers know the details of some of the components present in the model and they have moderate knowledge about the model. In the white box model, the attacker has complete knowledge about this model and this scenario happens only in the worst case.

2.2. Adversaries goal

The adversaries' goal differs by means of the following classification. If an adversary conducts a targeted attack on the neural network that leads to misclassification means then it is known as integrity violation. If the adversary targets the system availability and makes it unavailable for a certain period of time means it is known as availability violation. If the adversary tries to compromise the confidential information then it is known as a privacy violation. The attacker conducts the attack mainly in two ways where one is a targeted attack and another one is a random attack. In the targeted attack, the adversary targets only a specific part of the training sample to yield an incorrect output. In the random attack, the attacker focuses on any part of the training sample and the goal is to misclassify the output result.

2.3. Types of cybersecurity attacks

Denial of service attack (DoS): It is conducted by sending a large amount of traffic to the intended recipient, such that they will be no longer allowed to access the service from the corresponding PC. The main intention of this attack is to freeze or stop the service permanently or temporarily [21].

Remote to local attack: The attackers take advantage of the system using the network connection and conducts attacks by means of the vulnerabilities(bugs) already existing in the system. In the local attack, the attackers carry out unauthorized access to the system by using their already existing account to the system. The remote attacks are easier to prevent, but the local attacks are hard to detect. The attackers send a packet between the network and machines during remote to local attacks. The vulnerability of machines is exploited [22].

Probing: The networks are scanned by the attackers and they easily collect the information and data [23]. The machines and their services are mapped by the attackers.

User to root attack: The system and normal user account are easily traced by the attackers. Especially, the passwords are traced and the user data may be lost [24].

Adversarial Attacks: Adversarial attacks raise questions about whether deep learning is suitable for privacy concerning applications. Xu et al. [25] presented an approach that considers the safety of text, image, and graphs used in the Deep Neural Network model. Because the bank often takes ID proof utilizing the photograph to check whether the customer is an authenticated person or not. If a bank offers a loan to an unauthorized person then it suffers a huge loss. Thus, the safety measures are critical in Deep Neural Networks. The adversary can hack the Deep Neural Network powered system by giving false inputs and causing the model to make misclassification. In the adversarial attacks, the attackers often insert perturbation similar to the training input used and these attacks are often white-box attacks. The protection mechanisms used against the white box attacks often have limited success. Katzir and Elovici [26] presented an approach to overcome this attack with defensive distillation and targeted gradient sign method and they also analyzed the problems associated with these methods. p-tampering is an attack conducted against learning algorithm by integrating a dreadful malicious noise in it. Here the attacker modifies the training data which has a probability p, but he is allowed to only select the adversarial samples with accurate labels. Saeed Mahloujifar et al. [27] used the bias attack mechanism to overcome the problem by increasing the value of the real-valued function.

Poisoning and Evasion attacks: In the training phase of deep learning poisoning attacks are conducted. To decrease the prediction accuracy of the deep learning algorithm, the adversary inserts the virus into the training samples. Evasion attack is mainly targeted towards the prediction process of deep learning. Here a wrong input is given to the neural network by the adversary to yield a wrong classification result. In both attacks, the attacker can control the input data. Jiang et al. [28] used Particle Swarm Optimization(PSO) algorithm to overcome the poison and evasion attacks by focusing on the training phase in case of poison attacks and interference phase in case of evasion attacks. They observed a classification accuracy decline from 95% to 33% for poison attacks and a 93% to 22% decline for evasion attack when injected with malware samples. The Convolutional Neural Network which takes input in the form of the image is often subjected to evasion attacks. The attacker conducts these attacks by injecting pixels level perturbations inside the image. The problem widely occurs

in License plate recognition where the perturbations are inserted to alter the number of the license plate. The attackers often modify the images in a way in which it cant be seen by the naked eye. Yaguan Qian et al. (2020) took this problem as an intricate optimization problem that needs to be solved and they applied a genetic algorithm for this. The adversarial perturbation is identified by this algorithm. The authors indicate that this problem needs further exploration since it is a complex problem to be solved.

Integrity Attacks: Integrity attacks are mainly focused on altering or corrupting the data that resides on the system. The attacker mainly conducts this attack by encrypting the organization's important details by asking a huge theft of money to decrypt it. Guangyu et al. (2017) presented an optimal switching data integrity attack. Here an attacker compromises a problem-free system by partially inserting the malware into the selected components and continuously conducting a targeted attack by switching in between different systems. The authors aimed to find an optimal attack sequence of the compromised actuator by using limited energy to improve the quadratic performance.

Causative Attacks: The causative attack is mainly conducted by targeting the decision-making algorithm to yield an inaccurate classification of the neural network. This shows that most of the estimation algorithms are prone to causative attack. To overcome this problem Sihag and Tajer [29] proposed a secure parameter estimation algorithm that can detect the attack and isolate the neural network model. The summary of the cybersecurity attacks held is provided in Table 1.

3. Deep learning and its classification trend of cybersecurity

The most important subsection of machine learning is the deep learning technique. The classification of deep learning based on the cybersecurity attacks is shown below. The classifications of deep learning are portrayed in Fig. 2 and its subsections are discussed in the below sections.

3.1. Convolutional Neural Network (CNN)

The feed-forward neural network of CNN consists of convolutional, multiple hidden layers, pooling, and fully connected layers respectively. The elements are represented using neurons and the array can store all the inputs. The arrays are two and three dimensional in nature. Generally, the fundamental element of CNN is a convolutional layer [31]. The original input is the convolutional kernel which is the representation of weight also the receptive field is a smaller window [32]. The feature map is obtained from the input calculation. The basic structure of the convolutional neural network is illustrated in Fig. 3. The CNN based cybersecurity attack detection is divided into single CNN, Multi-CNN, Variants of CNN, Acoustic model of CNN, and Limited Weight Sharing of CNN.

3.1.1. Single CNN

The deep security attack detection method adopts one single CNN and the supervised training process is performed [33]. During security image recognition, the three-dimensional alignments are carried out in the 9th layer of CNN. There is no other weight sharing is proceeded in the presence of many local connected CNN layer [34]. The effective training set is predicted from the bootstrapping procedure of the web-scale. The performance of cybersecurity attack detection is improved using a few schemes such as discriminative feature learning, feature fusion, novel learning algorithms, loss function designing, and accepting exact activation.

3.1.2. Multi-CNN

The deep features are analyzed with multi-CNN, here more than one CNN is used. It is mainly used to amalgamate the features effectively. The deep features are extracted from the various input and different environmental conditions. Each CNN is trained by extra CNN also the performance is enhanced [35]. The feature extraction from different region and aspects are the basic operation of multi-CNN. Therefore, data computing and collection requires important efforts. The features of the different malware can be extracted using this technique.

3.1.3. Variants of CNN

The different kinds of variants used in CNN to enhance the performance of the system is derived as follows. Therefore, the computational load and parameters are reduced by using down-sample [36]. Many CNN layouts are designed and modified using kernel function.

3.1.4. Acoustic model of CNN

The shared weight, receptive field, and spatial sampling data are combined and used for acoustic CNN. The additional joining of max pooling and convolutional layers are also used in the new environment to adapt to the tasks easily [37]. The time axis is implemented for data convolution with no validations. The local correlations are captured in the presence of weight sharing also the equivalent variances of CNN are collected.

3.1.5. Limited weight sharing of CNN

The performance of CNN is improved by adding a limited amount of weights during the pre-training process [38]. The similar feature mapping with weight sharing is performed among the neurons. During weight sharing procedure, similar pooling layers are connected with the conventional layer [39]. The features are calculated using neurons as well as the amount off parameters is increased rapidly. The better initial value is obtained during the weight training procedure and the pooling layer can sub sampled the learned values.

3.1.6. Cybersecurity applications using CNN

Zhang et al. [40] presented a CNN based model for network intrusion detection which identifies the malicious activities that take place on the internet. Here, they are using a new Class Imbalance Processing Technology(SGM-CNN) for large scale datasets which consist of both undersampling(Gaussian Mixture Model) and oversampling(Synthetic Minority) schemes. The intrusion detection datasets usually suffer from an unbalanced class problem, that offers a low detection rate. The CIPT technique improves the classification accuracy of minority classes and provides a detection rate of 99.85%. Xiao et al. [41] proposed a malware classification framework to classify the different types of malware and their malicious intent. It first visually analyze the malware and then the classifier extracts the features for classification. The malware present in binary form is visualized using entropy graphs and the Deep CNN(DCNN)s used for feature extraction. The accuracy of this approach is 0.997 for the Malimg dataset and 1 for the Microsoft dataset.

3.2. Autoencoder (AE)

One or more hidden layers with input and output layers are connected to the Autoencoder(AE). The AE consists of a similar amount of input and output as well as the data transmission is carried out by a smaller path. The transfer and unsupervised learning issues are solved using a neural network. Therefore, task discovery and analysis are performed with the usage of autoencoders based on their characteristics [42]. The encoder and

Table 1
Summary of cybersecurity attacks.

Author Name and Year	Name of the attack	The intention of the attack	Demerits	Type of Neural Network/technique applied
Sihag and Tajer [29]	Causative Attack	To alter the decision of the algorithm	Computational Complexity, Attack Complexity	Decision-Making Algorithm
Guangyu et al. (2017)	Integrity Attack	To insert false information to partial actuators		Cyber–physical system
Yaguan Qian et al. (2020)	Spot Evasion Attack	To generate malicious images resembling the original images	Serves as a big threat for the License Plate Identification system	Convolutional Neural Network
Jiang et al. [28]	Poison and Evasion attack	To reduce the classification accuracy by injecting malware	These attacks significantly decrease the classification accuracy	Deep Neural network, PSO
Mahloujifar et al. [27]	Poisoning attack	To increase the error probability	It does not apply to strong p-budget attacks	Probably approximately correct learning
Katzir and Elovici [30]	Adversarial attack	To compute the networks loss gradient	The complex tradeoff for future research and increased cost	Neural Network
Xu et al. [25]	Adversarial attack	Attacker targets the deep learning model to make mistakes	Safety-Critical applications are widely affected by these attacks	Deep Neural network

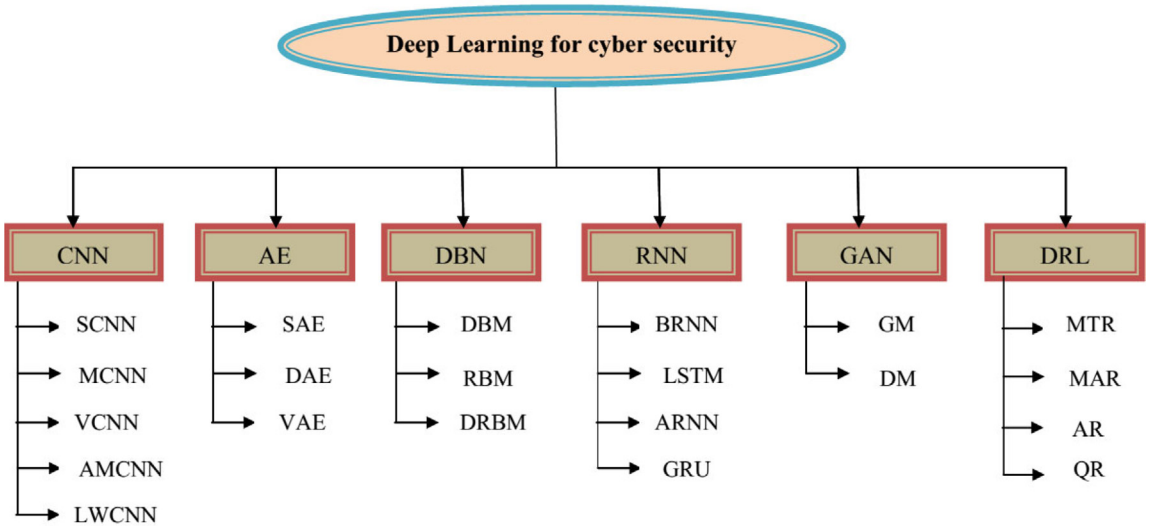

Fig. 2. Classification of deep learning based on cybersecurity.

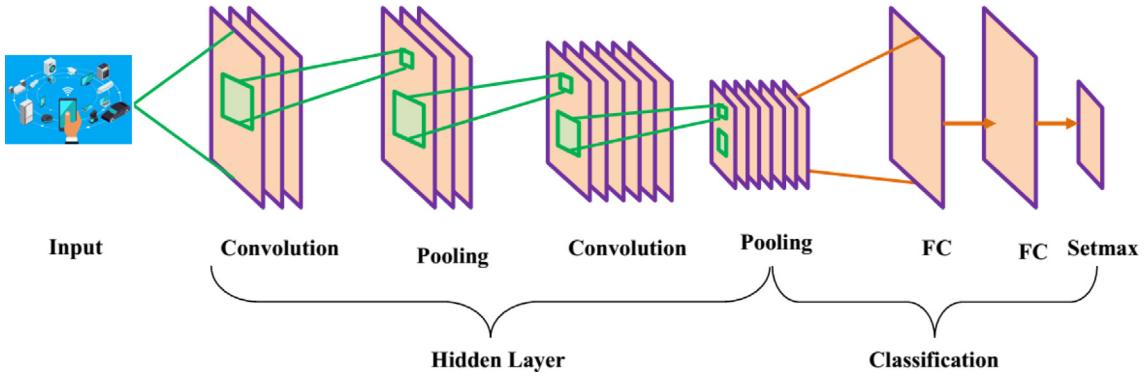

Fig. 3. Structure of convolutional neural network.

decoder are the fundamental components of the autoencoder. Hence, the inputs are received by the encoder and fed to the novel model (i.e. Latent or Code). The encoder distributes a code to the generator and the reconstructed errors are reduced through the training procedure of autoencoder. The basic architecture of autoencoder is depicted in Fig. 4 as well as the minimum input and output differences are shown effectively. The stacked,

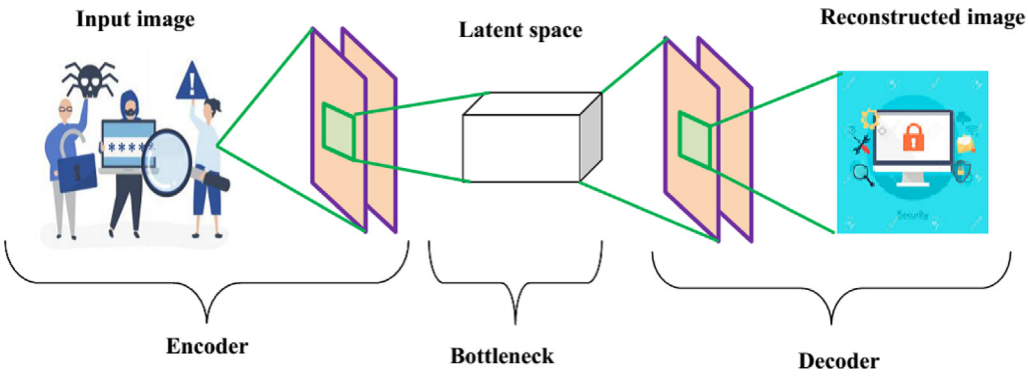

Fig. 4. Organization of Auto Encoder.

denoising and variational autoencoder are the few kinds of the autoencoder.

3.2.1. Stacked Auto Encoder (SAE)

The stacked encoder is one of the unsupervised learning of autoencoders. The input, output, and hidden layer are the three basic layers of the stacked autoencoder [43]. The representation of the hidden layer is used to map and reconstruct the input data. In each turn, the training process is executed via a greedy layer selection method. The final feature from the last layer is to perform the supervised learning procedure. The forward order running is to execute the autoencoder process as well as the reverse order is to execute the decoder process. Thus, the higher-order feature delivers vector input. Ultimately, the softmax is used to solve the classification issues effectively.

3.2.2. Denoising Auto Encoder (DAE)

Similar input and output data are used for the autoencoder process [44]. The noise has been added to the training procedure and it produces denoising power. The denoising autoencoder can train all convolutional kernels also the auto coder is trained. In classification, the optimal feature and denoise input are obtained.

3.2.3. Variational Auto Encoder (VAE)

The important generative representation of variational encoder was introduced in the year of 2013. The backpropagation has been lead to semi-supervised learning and quick training process [45]. It is suitable for the application of IoT device security, sensor failure detection, and the security of the intrusion systems respectively [46]. The probabilistic model of learning is perfectly implemented using a variational autoencoder. The visualization, recognition, representation, and denoising task are executed by the variational autoencoder.

3.3. Deep Belief Network (DBN)

The stochastic and hidden layer is a basic component of the deep belief networks. The stochastic variables with a direct acyclic graph are used to implement DBN [47]. The generative and discriminative DBN are worked under the principle of greedy selection. The unobserved variables and learning problems are important issues in DBN [48]. During posterior distribution with the training, the procedure is complex. Hence, the states of 0 and 1 are used as binary units for the stochastic model. The structure of the deep belief network is shown in Fig. 5 and its classifications are explained in the below section.

3.3.1. Deep Boltzmann Machine (DBM)

The stacked layer of restricted Boltzmann machine with graphical, unsupervised, generative, and probabilistic representation is used in DBM. The data latent features are detected with the usage of DBM and it contains an undirectional connection [49]. The greedy layer is used to perform an effective learning and parametric inference procedure. The optimal parameters are detected using unsupervised representation.

3.3.2. Restricted Boltzmann Machine (RBM)

The most popular type of deep belief neural network is the restricted Boltzmann machine. The stochastic binary unit and edges are the part of a stochastic neural network [50]. Hence, the scalability and impractical issues are aroused during the Boltzmann machine learning process. The neurons from the RBM creates a bipartite chart with each visible hidden layers are connected together [30]. A similar layer connection is restricted with the process are executed using an effective algorithm. The dimensionality minimization and feature learning are performed via RBM.

3.3.3. Deep Restricted Boltzmann Machine (DRBM)

The improved power with deep belief and Boltzmann network are the combinations of deep restricted Boltzmann machine [51]. The higher quality features are extracted using DRBM. Each layer is strictly restricted by DRBM. The combination of the deep and restricted network can organize each layer [52]. During the training process, each data with gradient and free energy computations are carried out.

3.4. Recurrent Neural Network (RNN)

The one or more feedback connection is associated with the recurrent neural network and it functions as a loop activation. The sequence learning and temporal procedures are performed via the enabled network [53]. The additional loop with multi-layer Perceptron is a basic of RNN and it consists of smaller memory. The activation of stochastic function with neuron is connected potentially [54]. The same gradient descent function is used to execute learning, activation, and architectural functions. The recurrent features are collected through annealing concept. The recurrent neural network structure is depicted in Fig. 6.

3.4.1. Bidirectional RNN (BRNN)

The ordinary RNN limitations are improved using bidirectional RNN [55]. At a specified time with past and future input is used to train the BRNN. The structure is divided into forwarding and backward states. The backward state does not have the input connection of forwarding state output [56]. A similar network takes time and the objective functions are minimized effectively.

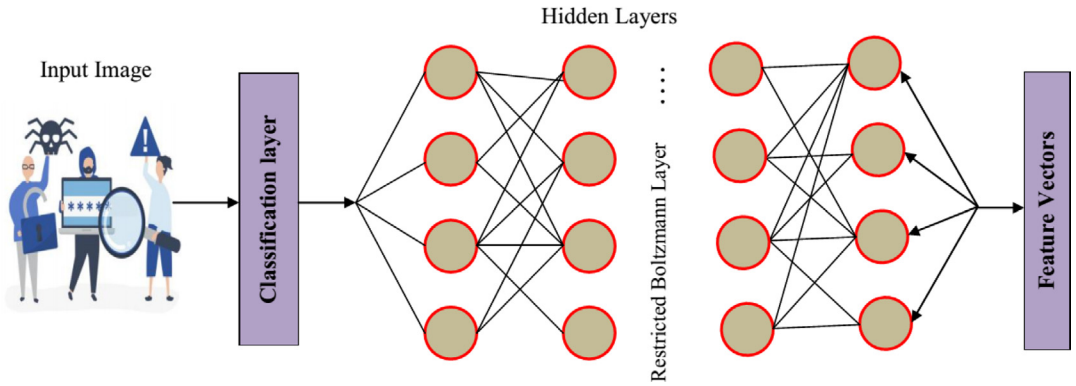

Fig. 5. Structure of deep belief network.

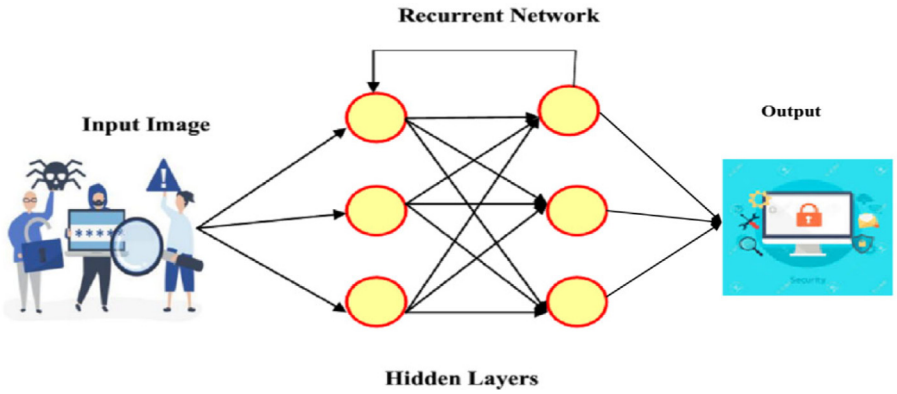

Fig. 6. Structure of recurrent neural network.

Future information did not require any delays. The complications of forwarding and backward connections are fed through backpropagation.

3.4.2. Long Short Term Memory (LSTM)

The elaboration factor of RNN is represented as long short term memory. The input of 0 and 1 are used for every computing gate units [57]. The feedback information is saved with the help of LSTM and all the LSTM consist of several neurons. Here, the write, read, and forget are the memory gates [39]. The memory cells are controlled using these gates. The training stage with backpropagation is affected by the issue of vanishing.

3.4.3. Acoustic model of RNN (ACNN)

The acoustic model consists of lengthy vector data and temporal variability. Thus, the long term dependency data are not captured by CNN [58]. The vanishing issues easily affect these networks. The exponential error and decay function are carried out because of backpropagation. The unacceptable arrangement of weights is adopted easily. The dimensionality minimization and feature learning are extracted quickly.

3.4.4. Gated recurrent unit

The long term dependency during the RNN training process is predicted using the gated recurrent unit (GRU). The hidden layer with the state to state transmission is modified besides a few variations in LSTM are to produce GRU [59]. Therefore, the representation of simplicity and popularity is the major reason. Hence, few parameters are required in GRU and the network operations are performed easily.

3.5. Generative Adversal Network (GAN)

The generator and discriminator is a major model of GAN. The tasks are determined by means of the discriminator model as well as the accurate output is produced using discriminator [37,60]. The real and artificial input and outputs are correctly recognized using GAN. The high quality and synthetic data are created [61]. The new data obtained from the former network. The real and fake data in a latent network is clarified by the discrimination process. Hence, the minimax theory is the major objective function of GAN [62]. The discriminator and generator operations of GAN are expressed in Fig. 7.

3.6. Deep Reinforcement Learning (RIL)

In the year of 2015, deep mind reinforcement learning was introduced by Mnih et al. [22]. The cumulative rewards are maximized also it is the basic idea of the machine learning function. The high dimensional input data sizes are minimized by means of deep neural networks [63]. The values of Q- functions are implemented using multi-layer Perceptron. The deep reinforcement learning procedure is described in Fig. 8.

3.6.1. Multi-task reinforcement (MTR)

The powerful characteristic of reinforcement requires a time of learning and the number of trajectories respectively [48]. The performances are notably improved using the multi-task reinforcement learning method [64].

3.6.2. Multi-agent reinforcement (MAR)

The multiple agent reinforcement is operated with the amalgamation of optimal rewards. Hence, the arrays of multiple tasks are implemented quickly using MAR [65].

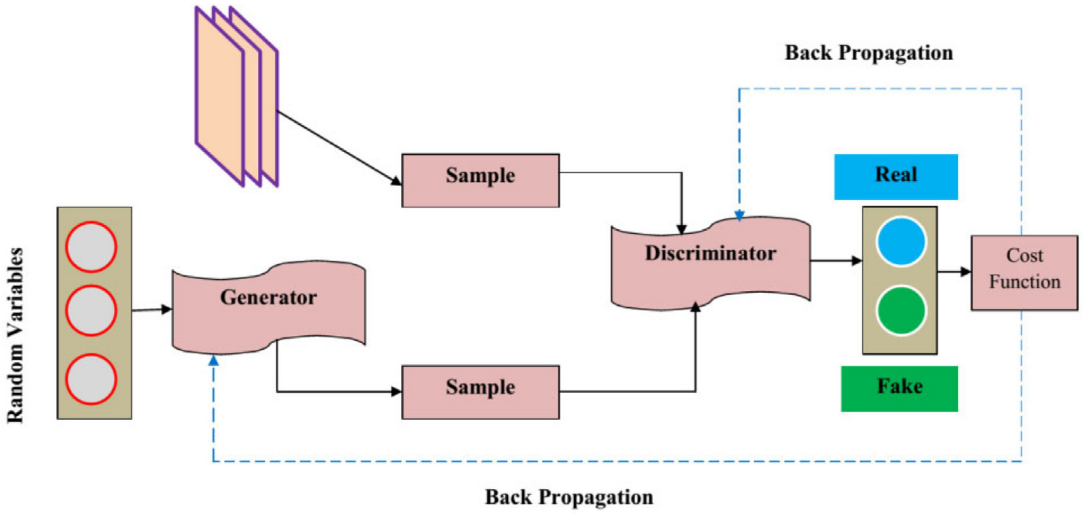

Fig. 7. Structure of generative adversal network.

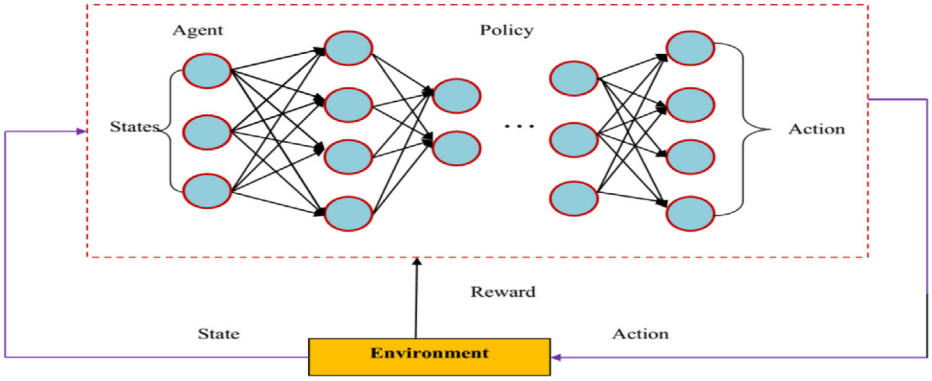

Fig. 8. Organization of deep reinforcement learning network.

3.6.3. Asynchronous reinforcement (AR)

The longer time period of deep reinforcement learning is an important problem [66]. So the asynchronous architecture is used to enhance the performance of deep reinforcement learning as well as the major parameters of servers are central and learning process [67].

3.6.4. Q-learning Reinforcement (QR)

Here, the temporal difference (TD) learning is the chief learning set of the Q-learning process also the entire environmental knowledge is never needed [24]. In every state, the optimal action solution is captured by using a traversed state [68]. The factor of Q is updated during the incremental process of the neural network also the memory space covered the previous-state values.

4. Analysis and discussion

The cybersecurity system is used to detect different kinds of attack based on deep learning method, which is discussed in this survey. The cybersecurity issues are occurred in everywhere for example mails, computer systems, vehicles, entertainments, banks, companies, financial institutions, online data storage, etc... In this survey, we chose a deep learning-based cybersecurity attack detection concept. There are approximately 80 papers are selected interrelated to the survey topic. The effectiveness of this survey is analyzed and compared using various parameters. In this section, the different kinds of algorithms, methods, platforms, advantages, and disadvantages based on the deep learning in cybersecurity attack detection papers are discussed effectively. Therefore, the general acronyms of this survey are listed in Table 2.

4.1. Performance analysis of cybersecurity attack detection papers

Kravchik and AsafShabtai [69] used 1Dimensional CNN to analyze the different types of cyberattacks held in Industrial Control Systems. Out of 36 cyber attacks present in the dataset, their proposed method successfully identified 31 types of cyber-attacks using convolutional and recurrent neural networks. They used the Secure Water Treatment(SWaT) dataset and implemented it under the GoogleTensorflow framework platform. However, this technique suffers from low interpretability and fails to identify the other five types of cyberattacks present. Mimura and Tanaka [70] created a generic detection approach that is free from any attack methods and feature vector. The main intention of this technique is to identify the adversaries' communication from the proxy server logs. It identifies two attacks namely command and control traffic and unfamiliar drive-by download attack with an F-measure value of 0.98 and 0.99. Vinayakumar et al. [71] categorized the cyber attacks into two levels namely network and host level. They focused on the dynamic malicious attack and large volumes of the dataset used when designing the Intrusion Detection System(IDS). However, this technique suffered from a high computational cost.

Vasan et al. [72] presented a CNN approach for image-based malware classification. This approach can identify different types

Table 2
List of Acronyms in cybersecurity with Deep learning concept.

Abbreviations	*Detailed Form*
AI	Artificial Intelligence
DL	Deep Learning
IoT	Internet of Things
CNN	Convolutional Neural Network
AE	Autoencoder
DBN	Deep Belief Network
GAN	Generative Adversal Network
RNN	Recurrent Neural Network
LSTM	Long Short Term Memory
SCNN	Singular Convolutional Neural Network
MCNN	Multi-convolutional Neural Network
VCC	Variants of Convolutional Neural Network
ACNN	Acoustic model of Convolutional Neural Network
LWCNN	Limited Weight Sharing of Convolutional Neural Network
SAE	Stacked Auto Encoder
DAE	Denoising Auto Encoder
VAE	Variational Auto Encoder
DBM	Deep Boltzmann Machine
RBM	Restricted Boltzmann Machine
DRBM	Deep Restricted Boltzmann Machine
GRU	Gated Recurrent Unit
ARNN	Acoustic Model of RNN
LSTM	Long Short Term Memory
BRNN	Bidirectional Recurrent Neural Network
ML	Machine Learning
TD	Temporal Difference
RIL	Deep Reinforcement Learning
QR	Q-learning Reinforcement
MAR	Multi-Agent Reinforcement
MTR	Multi-Task Reinforcement
AR	Asynchronous Reinforcement
UK	United Kingdom
DoS	Denial of Service
DBN	Deep Belief Network

of malware and classify it based on their family. The data variance challenge is overcome here using an augmentation technique. This approach suffers from a slightly higher run time overhead. Li et al. [61] presented an anti-steganalysis using CNN for detecting malware in images. They focused on the Least Significant Bit based evolutionary algorithm attack and gradient-based attack. It shows significant ways to compromise the steganalysis and the weakness of the neural network. The summary of the cybersecurity attacks that take place in the CNN network is provided in Table 3.

The summary of the cybersecurity attacks that take place in AE powered neural networks is shown in Table 4. Meira et al. [80] used an unsupervised model of learning to detect unfamiliar attacks by using an anomaly-based IDS. This method has better performance and it is appropriate for the IDS, but the false positive rate is high. Experimentally, NSL-KDD datasets are used and the Python software is used for implementation. Thing [81] focused on the security of IEEE 802.11 and identified the novel threats and attacks conducted on it. To identify and classify the anomalies they used an unsupervised Deep Learning Approach. The dataset used is AWID-CLS dataset and the approach is implemented using. Even though the classification performance is accurate, it has a large computational cost. Lopez-Martin et al. [82] proposed an IDS system to identify the malicious labels present inside the decoder layer using a conditional variational autoencoder. It can create effective feature reconstruction and provides higher classification results. However, this method offered lower classification results. It is implemented in the OMNET platform using an STL-10 dataset. Diro and Chilamkurti [21] identified the cyberattacks held in the IoT environment and mainly focused on zero-day attacks. They analyzed the hidden patterns present in the training data to separate the malicious traffic from normal traffic. The experiments are performed using JAVA software and the detection process is centralized but not applicable to analyze huge parameters.

In [83], the supervised technique has improved outcomes in classification but is not appropriate for maximizing other stages. The dataset of NSL-KDD is implemented with the usage of the Python platform. In [84], the author used the unsupervised learning process. This method is more scalable and flexible but not suitable for conducting a massive experiment. The performance of their proposed concept is analyzed using gearbox datasets and implemented in the C^{++} programming language.

The cybersecurity attack papers focused on the deep belief network are discussed in Table 5. Skopik et al. [86] discovered that to prevent future networks from attacks, the information sharing between two organizations should be secured. Even though it offers a secure information sharing, it is costly and deployable only in critical infrastructures. Zhang et al. [90] presented a DBNB and support Vector Machine powered network IDS system. Balakrishnan et al. [103] developed an Intelligent IDS using DBN to overcome the critical cyber attacks held in the IoT environment. The main intent of this model is to identify the adversary's activity inside the network, once they enter the border. This model can identify the data injection attacks precisely when trained with the MNIST dataset. However, this model suffered from high computational cost and low accuracy. Thamilarasu and ShivenChawla [88] also proposed an intelligent IDS for IoT systems using deep learning algorithm to identify the malicious traffic. This method is more effective and feasible with a larger bandwidth. The dataset used is NSL-KDD and it is implemented in Matlab. The author used NSL-KDD, MNIST, and Kyoto datasets for the unsupervised deep learning process and predicted the denial of service, and overflow attacks efficiently. Even though this method offers high accuracy, complex hardware implementation is required.

The recurrent neural network papers about cybersecurity attacks are represented in Table 6. Nabil et al. [91] used the deep feed-forward neural network and RNN to identify the consumers who report false electricity usage. This mainly happens in the Advanced Metering Infrastructure(AMI) and it is also known as electricity theft cyber Attack. This approach is implemented in realtime detectors using the Python platform to detect the contamination attacks. Venkatraman and Vinayakumar [96] presented a hybrid deep learning architecture to detect the malware in images. The main intent is to identify suspicious behavior along with the different hybrid architectures. The Malimg, VirusSign, and VirusShare datasets are utilized for malware detection and the procedure is implemented in both Java and Python. The outputs are often subjected to misclassification in this approach. In [92], the supervised model used has parallel computation but low translation and encoding operations. The C^{++}languaging program is used with the COCO dataset for training. In [93], the unsupervised learning model with the SST dataset is implemented by JAVA software. This method contains a Better forward procedure and it is complex for huge data analysis. Salehinejad et al. [95] suggested a supervised model with the BABL dataset and OMNET platforms are used. It is the simple and flexible but larger time needed during weight transfer.

The cyber security attacks based on deep reinforcement learning is presented in Table 7. In [22], presented an unsupervised learning process with the CIFAR-10 dataset, and JAVA software is used. This method is suitable for asynchronous demon attack detection employing lower training speed. Allen and Liu [99] proposed a Monte Carlo Bayesian Reinforcement learning to reduce the median estimated learning time and provide faster learning. The cost of the system implementation is particularly high per host and also while identifying the current threats in the system.

Table 3
Convolutional neural Network for cybersecurity attack detection.

References	*Learning Model*	*Platform*	*Attacks*	*Disadvantage*	*Dataset*
[69]	Unsupervised	Google Tensorflow framework	Zero-day attack	Interpretability of attack detection is low	SWaT
[73]	Unsupervised	Apache spark cluster	Denial of service and distributed denial of service	High computational cost	KDDCup 99 [74]
[70]	Supervised	Python 2.7	–	Low-performance accuracy	MWS [75]
Tariyal et al. (2016)	Unsupervised	Java	Phishing attack	Data missing occurred due to noise	NIDS [76]
[40]	Unsupervised	Python	Web attacks(Brute Force, SQL injection, and XSS), Infiltration, Heartbleed, Backdoor, and worms.	The multiple convolutional layers present increases the computational time and cost	UNSW-NB15 [77], CICIDS2017 [78]
[41]	Unsupervised	Keras with TensorFlow	Malware attacks (Worm, Trojan, Backdoor, etc.)	Fixed Segment length, Overfitting problem, and Performance Degradation	Malimg (https://www.kaggle.com/afagarap/malimg-dataset) and Microsoft from Kaggle
[72]	Unsupervised	Python	Cyberattack(trojan, backdoor, worm)	Runtime overhead	Mailmg, and IoT android mobile dataset
Shiyu Li et al. (2020)	Unsupervised	–	Evolutionary algorithm attacks, and Gradient-based attacks	Perturbations during backpropagation	BOSSbase [79]

Table 4
Auto Encoder Network for cybersecurity attack detection.

References	*Learning Model*	*Platform*	*Attacks*	*Disadvantage*	*Dataset*
[80]	Unsupervised	Python	Unfamiliar attacks	The high false-positive rate	NSL-KDD [74]
[81]	Supervised	Matlab	Novel threats and attacks	High cost	AWID-CLS [85]
[82]	Supervised	OMNET	Denial of service	The lower performance of classification	STL-10 (https://ai.stanford.edu/~acoates/stl10/)
[21]	Unsupervised	Java	Zero-day attack	Not suitable to huge parameter	NSL [74]
[83]	Supervised	Python	–	Not suitable to optimize many layers	NSL-KDD [74]
[84]	Unsupervised	C++	–	Not suitable for a huge experiment	Gearbox

Table 5
Deep Belief Network for cybersecurity attack detection.

References	*Learning Model*	*Platform*	*Attacks*	*Disadvantage*	*Dataset*
[86]	Unsupervised	Web	Covert Cyberattacks	Critical infrastructure	ENISA (http://data.europa.eu/88u/dataset/enisa-threat-taxonomy-1)
[87]	Unsupervised	Matlab	Sinkhole attack	Larger width	NSL-KDD [74]
[88]	Supervised	Raspberry pi	Denial of service and overflow attack	The high cost of computation	Traffic dataset [88]
[89]	Unsupervised	C++	User root attack, remote to local attack and probe attack	High hardware requirement	NSL-KDD [74], MNIST,and Kyoto [76]
[90]	Unsupervised	–	Network intrusion attack	Needs improvement in accuracy	CICIDS2017 [78]

The dataset is composed of collecting malicious emails and the system is implemented using a LINUX platform. Nguyen and JanapaReddi [94] reviewed the widely used Deep Reinforcement Learning(DRL) models to identify the cyber attacks in the system. The DRL technique is widely used to solve the dynamic, intricate, and multidimensional security problem with a limited amount of communication. Ferdowsi et al. [100] presented a DRL algorithm for autonomous vehicles to safeguard it from the cyber–physical attacks. A game theory model is created between the adversary and the Autonomous vehicle. Here the adversary injects malicious data to the autonomous vehicle's sensor to alter the optimal spacing and result in accidents. This system safeguards such an attack by minimizing the adversaries' spacing deviation. Yu et al. [101] used DRL to combat real-time attacks such as illegal woodcutting,

Table 6
Recurrent Neural Network for cybersecurity attack detection.

References	*Learning Model*	*Platform*	*Attacks*	*Disadvantage*	*Dataset*
[91]	Semi-supervised	Python	Contamination attack	Not suitable to hyper parametric analysis	ENISA (http://data.europa.eu/88u/dataset/enisa-threat-taxonomy-1)
[92]	Supervised	C++	–	Lower translation and encoding	COCO [92]
[93]	Unsupervised	JAVA	–	Complex for huge data analysis	SST [94]
[95]	Supervised	OMNET	–	A larger time occurred during weight transfer	BABL [95]
[96]	Supervised	Apache Spark	Malware attack	Low performance	Malimg (https://www.kaggle.com/afagarap/malimg-dataset)
[71]	Supervised	Python	Malware attack	High cost	Ember, MalConv [73]
[97]	Unsupervised	Python	Zero-day attack	Damages occurred due to misclassification	Malimg (https://www.kaggle.com/afagarap/malimg-dataset)

Table 7
Deep Reinforcement Learning Network for cybersecurity attack detection.

References	*Learning Model*	*Platform*	*Attacks*	*Disadvantage*	*Dataset*
[22]	Unsupervised	JAVA	Demon attack	Low training speed	CIFAR-10 [98]
[99]	Semi-supervised	LINUX	Denial attack	High cost	Email [99]
[94]	Unsupervised	OMNET	Adversarial attack	Only a limited amount of communication attacks are detected	SST [94]
[100]	Unsupervised	Apache Spark	–	Temporal features only extracted	FLIR [100]
[101]	Semi-supervised	Double Oracle Framework	Yolo attack	A limited number of iteration	SSE [101]

Table 8
Generative Adversal Network for cybersecurity attack detection.

References	*Learning Model*	*Platform*	*Attacks*	*Disadvantage*	*Dataset*
[23]	Unsupervised	MATLAB	Denial attack	Noise during overlap	CIFAR-10 [98]
[30]	Supervised	C++	Partitioned attack	Not suitable for various tasks	Malwr (https://malwr.com)
[102]	Semi supervised	LINUX	–	Computational complexity	NSL-KDD [74]
[102]	Supervised	Patching	–	Complex security detection	SSE [101]
[102]	Supervised	JAVA	Zero-day attack	Does not consider information based on network payload	ISCX Botnet [102]

poaching, and overfishing. By means of using the deep Q network, the attacker is identified by the realtime information obtained. Realtime information is derived by obtaining the foodprints of the illegal member.

Furthermore, the generative adversarial network for cybersecurity attack detection is tabulated in Table 8. Radford et al. [23] presented a Deep CNN-GAN pair to identify the set of malicious images. The unsupervised learning models have a hierarchical representation with noises occurring during a denial attack. The CIFAR-10 datasets are implemented using MATLAB platform. It has hierarchical representation with noises that occur during overlap. In, [30] the supervised learning model for malware identification using dynamic analysis using an up-to-date dataset known as Malwr. Hence, it provides empirical and classified evidence but it not suitable for different kinds of tasks. The partitioned attack is detected effectively using this approach.

Lin et al. [102] presented an IDS based GAN network which can create the adversarial attacks to compromise the IDS. The attack conducted is a type of black-box attack. The dataset used is NSL-KDD and is implemented in the LINUX platform. This method is highly robust against various kinds of attacks and it possesses high computational complexity. Chhetri et al. [104] presented a GAN security model to overcome the cross-domain attacks that takes place in the cyber–physical system environment. The Optimum availability and integrity performance are accomplished with complex security identification. The botnet attack is one of the large scale attacks that damage the cybersecurity. Yin et al. [105] presented a Botnet based GAN(bot-GAN) to overcome the malicious attacks and detect the new botnets. The mechanism is scalable and enhances botnet detection, but it never considers the payload information. The dataset of ISCX Botnet is used and the framework is implemented using JAVA software.

4.2. Comparative analysis

In this survey, approximately 101 papers are collected and 80 papers were taken for technical analysis. Each of the papers is

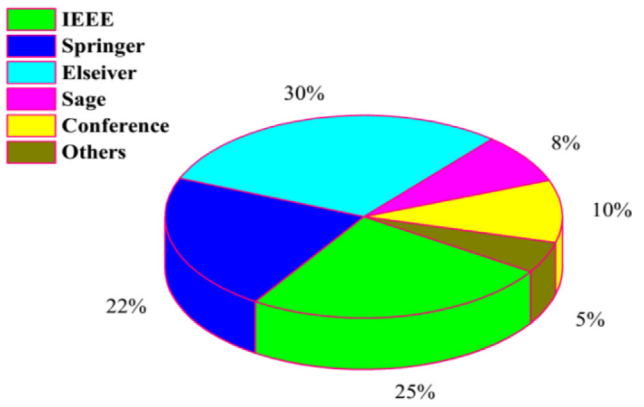

Fig. 9. Representation of cybersecurity attack detection papers chosen from different journals.

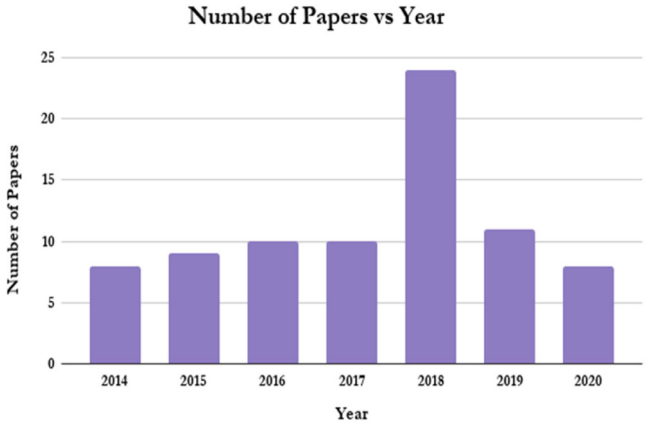

Fig. 10. Analysis of cybersecurity attack detection papers published every year.

referred to as the category of deep learning. The papers are selected from different kinds of journals such as Elsevier, Springer, IEEE, Sage, Conference, and others. The pie chart representation of papers selected from different kinds of journals is described in Fig. 9. From this, 30% of papers are selected from Elsevier, 22% of papers are selected from springer, 25% of papers are selected from IEEE, and 8% deep learning method papers are selected from the sage journals. Finally, the highest number of papers are chosen from the Elsevier journal, and the papers are collected from the cybersecurity and deep learning domain.

The cybersecurity attack detection papers which focus on deep learning are selected from the year 2014 to 2020. In this survey, we used approximately 80 papers for technical review. There are eight papers are chosen from 2014, nine papers from 2015, ten papers from 2016, twelve papers from 2017, twenty-four papers from 2018, and the remaining eighteen papers from the year of 2019. The highest number of papers are selected from the year 2018. Eight papers are taken from the year 2020. The number of papers chosen from every year is noted in Fig. 10.

In this paper, the cybersecurity attack detection based on deep learning methods is categorized into six classes such as Convolutional Neural Network (CNN), Auto Encoder (AE), Deep Belief Network (DBN), Recurrent Neural Network (RNN), GenerativeAdversal Network (GAN) and Deep Reinforcement Learning (DIL). We have selected 10% of papers from RNN, 7% of papers from AE learning, 8.5% of papers based on BBN learning, 8.2% papers from CNN learning, 3% of papers based on GAN learning, 4% of papers based on RIL learning and remaining papers are based on the concept of common deep learning. Several papers

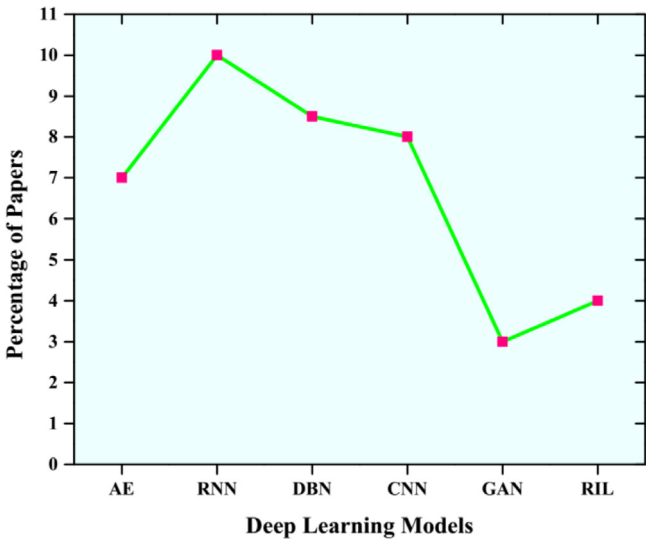

Fig. 11. Analysis of cybersecurity attack detection papers based on deep learning methods.

belong to the recurrent neural network domain. The number of papers published based on the deep learning types is represented in Fig. 11.

From this survey, the deep learning-based cybersecurity attack detection papers are published from various countries such as Italy, Turkey, India, USA, UK, Japan, Jordan, China, Nigeria, Israel, Switzerland, Pakistan, Taiwan, Canada, Russia, Australia, and others. Each of the countries has published more papers related to deep learning concepts and among them 30% of papers belongs to the United Kingdom (UK). The next 18% of papers are published by China. The lowest 1% percentage of papers are published by countries like Turkey, the USA, Jordan, Israel, Canada, and Russia. The analysis of the paper published by each country is represented in Fig. 12.

In this survey, we analyzed different kinds of attacks from the cybersecurity system using deep learning methods. The various kinds of attacks like denial of service, probe, malware, zero-day, phishing, sinkhole, user root, and others are discussed in the above sections. The number of papers chosen for every attack is formulated in Fig. 13. Here, we chose 12 papers for denial attack, 3 for probe, 5 for malware, 11 for zero-day, 5 for phishing, 2 for sinkhole, 5 for user root, and remaining papers for other attacks. Several papers are chosen for denial of service attacks.

5. Open issues and future research directions

All these survey papers were produced an effective deep learning method for security attack detection procedure. Each performance results such as accuracy, precision, recall, sensitivity, specificity, and acuteness are best and highly accepted but it contains few complications based on their method, platform, algorithms, etc... So the number of papers are introduced to solve these issues successfully and here a few of the open challengeable issues are scheduled as follows:

- The inputs are regularly managed by the deep learning algorithm. So the deep learning parameter, topology, and layer identification are complex.
- The researchers should also focus on problems like how an attacker uses the Deep learning technique to enter the victim's system which is already secured with deep learning techniques.

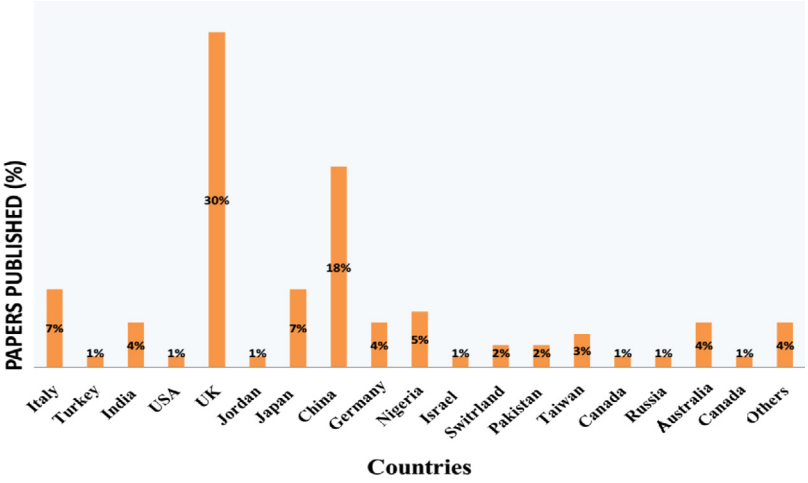

Fig. 12. Analysis of cybersecurity attack detection papers published by each country.

- To detect and classify an intrusion in the network one should always consider the type of attacks held and the classes to which it belongs. The deep learning methodology designed to solve cybersecurity problems should not be focused on a single problem(malware detection) alone. The deep learning model should be combined with multiple machine learning methodologies and encryption algorithms to identify a large area of attack vectors. In the future, multiple deep learning models can be integrated into parallel to improve performance.
- The performance is often deterred by the normal data to malware ratio used in the training dataset. The performance metrics of cybersecurity applications such as speed, suspension of data poisoning, storage consumption, True Positive Rate, and False Positive Rate should be analyzed to evaluate the efficiency of the cybersecurity application created.
- To obtain a real malware dataset is very hard in realtime and not an easier task to accomplish. The malware datasets available are mainly created by experimentation or reverse engineering of the virus. So, in the future, the research can be focused on experimenting with different open-source datasets and benchmark models.
- The deep learning technique related to cybersecurity has higher cost complexity associated with it during error solving. Because, the deep learning techniques are similar to black boxes, the main cause of the error is literally hard to identify. In the future, the underlying causes of the attacks should be analyzed in detail to design an active learning approach for cybersecurity applications.
- High performance, GPU, larger storage, low false-positive rate, and accurate information are the basic requirement of the resource.
- The larger resources analytics required highly scalable, low power consumption, flexible, and local bandwidth algorithms.
- Most of the designs are high computational cost, intractable, and complicated hyper parametric structure.

6. Conclusion

The rapid development of cybersecurity attack detection based on deep learning algorithms is summarized in this paper. The applications of deep learning in cybersecurity attacks are successfully discussed. In this survey, nearly 80 papers are selected from the year 2014 to 2019. Here, we introduced several architectures

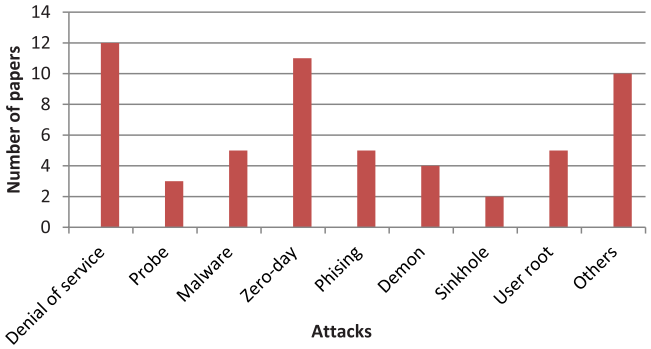

Fig. 13. Analysis of paper selected for each cybersecurity attack.

of deep learning methods and their applications. Each survey paper is collected from different kinds of journals such as Elsevier, IEEE, Springer, Sage, Conference papers, and others. Approximately 30% of papers were obtained from Elsevier journals and 10 of them were conference papers. Approximately 24 papers were selected from the year of 2018. Ultimately, the country of the United Kingdom published several papers. In the future, we plan to introduce an effective algorithm to solve the open issues challenges and design a robust cybersecurity application.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, et al., A view of cloud computing, Commun. ACM 53 (4) (2010) 50–58.
[2] M. Chen, S. Mao, Y. Liu, Big data: A survey, Mob. Netw. Appl. 19 (2) (2014) 171–209.
[3] Arwa Alrawais, Abdurrahman Alhothaily, Fog computing for the internet of things: Security and privacy issues, IEEE Internet Comput. 21 (2) (2017) 34–42.
[4] V. Sundararaj, Optimal task assignment in mobile cloud computing by queue based ant-bee algorithm, Wirel. Pers. Commun. 104 (1) (2019) 173–197.
[5] S. Vinu, S. Muthukumar, R.S. Kumar, An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks, Comput. Secur. 77 (2018) 277–288.

[6] V. Sundararaj, An efficient threshold prediction scheme for wavelet based ECG signal noise reduction using variable step size firefly algorithm, Int. J. Intell. Eng. Syst. 9 (3) (2016) 117–126.
[7] V. Sundararaj, Optimised denoising scheme via opposition-based self-adaptive learning PSO algorithm for wavelet-based ECG signal noise reduction, Int. J. Biomed. Eng. Technol. 31 (4) (2019) 325.
[8] V. Sundararaj, V. Anoop, P. Dixit, A. Arjaria, U. Chourasia, P. Bhambri, MR. Rejeesh, R. Sundararaj, CCGPA-MPPT: Cauchy preferential crossover-based global pollination algorithm for MPPT in photovoltaic system, Prog. Photovolt. Res. Appl. (2020).
[9] S. Russell, P. Norvig, Artificial intelligence: a modern approach, 2002.
[10] Wells, Lee Jaime, Camelio, Christopher Williams, Jules White, Cyber-physical security challenges in manufacturing systems, Manuf. Lett. 2 (2) (2014) 74–77.
[11] X.A. Larriva-Novo, M. Vega-Barbas, V.A. Villagrá, M.S. Rodrigo, Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies, IEEE Access 8 (2020) 9005–9014.
[12] Hsien-De Huang, TonTon, Hung-Yu Kao, R2-D2: color-inspired convolutional neural network (CNN)-based android malware detections, in: IEEE International Conference on Big Data, Big Data, 2018, pp. 2633–2642.
[13] S. Mahdavifar, A.A. Ghorbani, Application of deep learning to cybersecurity: A survey, Neurocomputing 347 (2019) 149–176.
[14] D.S. Berman, A.L. Buczak, J.S. Chavis, C.L. Corbett, A survey of deep learning methods for cyber security, Information 10 (4) (2019) 122.
[15] S. KP, M. Alazab, A comprehensive tutorial and survey of applications of deep learning for cyber security, 2020.
[16] Komal Jaswal, TanupriyaChoudhury, RoshanLalChhokar, SoorajRandhir Singh, Securing the Internet of Things: A proposed framework, in: IEEE: International Conference on Computing, Communication and Automation, ICCCA, 2017, pp. 1277–1281.
[17] Deng Li, Wang Gupta, Choi, A novel CNN based security guaranteed image watermarking generation scenario for smart city applications, Inform. Sci. 479 (2019b) 432–447.
[18] Kavukcuoglu Mnih, Rusu Silver, Bellemare Veness, Riedmiller Graves, Ostrovski Fidjeland, Petersen, Human-level control through deep reinforcement learning, Nature 518 (7540) (2019) 529.
[19] G. Parekh, D. DeLatte, G.L. Herman, L. Oliva, D. Phatak, T. Scheponik, A.T. Sharman, Identifying core concepts of cybersecurity: Results of two delphi processes, IEEE Trans. Educ. 61 (1) (2018) 11–20.
[20] G. Wu, J. Sun, Optimal switching integrity attacks in cyber-physical systems, in: 2017 32nd Youth Academic Annual Conference of Chinese Association of Automation, YAC, IEEE, 2017, pp. 709–714.
[21] Diro, Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Gener. Comput. Syst. 82 (2018) 761–768.
[22] Volodymyr Mnih, AdriaPuigdomenechBadia, Mehdi Mirza, Alex Graves, Timothy Lillicrap, Tim Harley, David Silver, KorayKavukcuoglu, Asynchronous methods for deep reinforcement learning, in: International Conference on Machine Learning, 2016, pp. 1928–1937.
[23] Alec Radford, Luke Metz, SoumithChintala, Unsupervised representation learning with deep convolutional generative adversarial network, 2015, ArXiv preprint arXiv:1511.06434.
[24] Cao Xiong, Q. Yu, Reinforcement learning-based real-time power management for hybrid energy storage system in the plug-in hybrid electric vehicle, Appl. Energy 1 (211) (2018) 538–548.
[25] H. Xu, Y. Ma, H. Liu, D. Deb, H. Liu, J. Tang, A. Jain, Adversarial attacks and defenses in images, graphs and text: A review, 2019, arXiv preprint arXiv:1909.08072.
[26] Z. Katzir, Y. Elovici, Gradients cannot be tamed: Behind the impossible paradox of blocking targeted adversarial attacks, IEEE Trans. Neural Netw. Learn. Syst. (2020).
[27] S. Mahloujifar, D.I. Diochnos, M. Mahmoody, Learning under p-tampering poisoning attacks, Ann. Math. Artif. Intell. (2019) 1–34.
[28] W. Jiang, H. Li, S. Liu, X. Luo, R. Lu, Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles, IEEE Trans. Veh. Technol. 69 (4) (2020) 4439–4449.
[29] S. Sihag, A. Tajer, Secure estimation under causative attacks, IEEE Trans. Inform. Theory (2020).
[30] Ziv Katzir, Yuval Elovici, Quantifying the resilience of machine learning classifiers used for cyber security, Expert Syst. Appl. 92 (2018) 419–429.
[31] Daming Li, Lianbing Deng, BrijBhooshan Gupta, Haoxiang Wang, Chang Choi, A novel CNN based security guaranteed image watermarking generation scenario for smart city applications, Inform. Sci. 479 (2019a) 432–447.
[32] Ma Li, Jiao, A hybrid malicious code detection method based on deep learning, Int. J. Secur. Appl. 9 (5) (2015) 205–216.
[33] Usama Ahmed, Imran Raza, Syed AsadHussain, Amjad Ali, Modelling cyber security for software-defined networks those grow strong when exposed to threats, J. Reliab. Intell. Environ. 1 (2–4) (2012) 123–146.
[34] Yaniv Taigman, Ming Yang, Marc Aurelio Ranzato, Lior Wolf, Deepface: Closing the gap to human-level performance in face verification, in: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 1701–1708.
[35] Xiong Zhao, Cheng Cheng, Zhou Li, Karlekar Xu, Shen Pranata, Xing, 3D-Aided Deep Pose-Invariant Face Recognition, in: IJCAI, Vol. 2, No. 3, 2018, p. 11.
[36] Junchi Zhang, Yue Zhang, DonghongJi, Mengchi Liu, Multi-task and multi-view training for end-to-end relation extraction, Neurocomputing 4 (2019a).
[37] Yu, Li, Recent progresses in deep learning based acoustic models, IEEE/CAA J. Autom. Sin. 44 (3) (2017) 396–409.
[38] Ossama Abdel-Hamid, Li Deng, Dong Yu, Exploring convolutional neural network structures and optimization techniques for speech recognition, Interspeech 11 (2014) 73–75.
[39] MdZahangir Alom, TarekTaha, Chris Yakopcic, Stefan Weisberg, PahedingSidike, Most ShamimaNasrin, MahmudulHasan, Brian C. Van Essen, Abdul A.S. Awwal, Vijayan K. Asari, A state-of-the-art survey on deep learning theory and architectures, Electronics 8 (3) (2019) 292.
[40] Hongpo Zhang, Lulu Huang, Chase Q. Wu, Zhanbo Li, An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset, Comput. Netw. (2020a).
[41] G. Xiao, J. Li, Y. Chen, K. Li, Malfcs: An effective malware classification framework with automated feature extraction based on deep convolutional neural networks, J. Parallel Distrib. Comput. (2020).
[42] Baldi, Pierre, Auto encoders, unsupervised learning, and deep architectures, in: Proceedings of ICML workshop on unsupervised and transfer learning, 2014, pp. 37–49.
[43] Jonathan Masci, Ueli Meier, Dan Ciresan, Schmidhuber, Stacked convolutional auto-encoders for hierarchical feature extraction, in: International Conference on Artificial Neural Networks, 2014, pp. 52–59.
[44] Yoshua Bengio, Li Yao, Guillaume Alain, Pascal Vincent, Generalized denoising auto-encoders as generative models, in: Advances in Neural Information Processing Systems, 2014, pp. 899–907.
[45] Xing Fang, MaochaoXu, ShouhuaiXu, Peng Zhao, A deep learning framework for predicting cyber attacks rates, EURASIP J. Inf. Secur. 1 (5) (2019).
[46] Yunchen Pu, ZheGan, Ricardo Henao, Xin Yuan, Chunyuan Li, Andrew Stevens, Lawrence Carin, Variational auto encoder for deep learning of images, labels and captions, in: Advances in Neural Information Processing Systems, 2016, pp. 2352–2360.
[47] Abdel-Rahman Mohamed, George E. Dahl, Geoffrey Hinton, Acoustic modelling using deep belief networks, IEEE Trans. Audio Speech Lang. Process. 20 (1) (2014) 14–22.
[48] Qin Zhang, Ou Yin, Zhang, A feature-hybrid malware variants detection using CNN based opcode embedding and BPNN based API embedding, Comput. Secur. 84 (2019b) 376–392.
[49] Bontupalli Alom, Taha, Intrusion detection using deep belief networks, in: 2015 National Aerospace and Electronics Conference, NAECON, 2015, pp. 339-344.
[50] Ugo Fiore, Francesco Palmieri, Network anomaly detection with the restricted Boltzmann machine, Neurocomputing 122 (3) (2014) 13–23.
[51] J. Yang, J. Deng, S. Li, Hao, Improved traffic detection with support vector machine based on restricted Boltzmann machine, Soft Comput. 21 (11) (2017a) 3101–3112.
[52] Ying Zhang, Peisong Li, Xinheng Wang, Intrusion detection for IoT based on improved genetic algorithm and deep belief network, IEEE Access 7 (2019c) 31711–31722.
[53] McDaniel Papernot, Swami, Harang, Crafting adversarial input sequences for recurrent neural networks, in: IEEE Military Communications Conference, 2016, pp. 49–54.
[54] Razvan Pascanu, Jack Stokes, MadyMarinescu HerminehSanossian, Anil Thomas, Malware classification with recurrent networks, in: IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, 2015, pp. 1916–1920.
[55] Hammed HaddadPajouh, Ali Dehghantanha, RaoufKhayami, Kim-Kwang Raymond Choo, A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting, Future Gener. Comput. Syst. 85 (2018) 88–96.
[56] Rosenberg Shabtai, Rokach, Elovici, Generic black-box end-to-end attack against state of the art API call based malware classifiers, in: International Symposium on Research in Attacks, Intrusions, and Defences, 2017, pp. 490–510.
[57] Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, Howon Kim, Long short term memory recurrent neural network classifier for intrusion detection, in: 2016 International Conference on Platform Technology and Service, 2016, pp. 1–5.
[58] Senior Sak, Rao, Beaufays, Fast and accurate recurrent neural network acoustic models for speech recognition, 2015, ArXiv preprint arXiv:1507.06947.

[59] Wei Feng, Yuqin Wu, Yexian Fan, A new method for the prediction of network security situations based on recurrent neural network with gated recurrent unit, Int. J. Intell. Comput. Cybern. 11 (4) (2018) 511–525.

[60] Jianhua Yang, Kai Liu, Xiangui Kang, Edward K. Wong, Yun-Qing Shi, Spatial image Steganography based on generative adversarial network, 2018, ArXiv preprint arXiv:1804.07939.

[61] S. Li, D. Ye, S. Jiang, C. Liu, X. Niu, X. Luo, Anti-steganalysis for image on convolutional neural networks, Multimedia Tools Appl. (2018b) 1–17.

[62] Dengyu Xiao, Yixiang Huang, Xudong Zhang, Haotian Shi, Chengliang Liu, Yanming Li, Fault diagnosis of asynchronous motors based on LSTM neural network, in: 2018 Prognostics and System Health Management Conference, 2018, pp. 540–545.

[63] Niyaz Javaid, Sun, Alam, A deep learning approach for network intrusion detection system, in: Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, 2016, pp. 21–26.

[64] AkankshaRai Sharma, PranavKaushik, Literature survey of statistical, deep and reinforcement learning in natural language processing, in: IEEE International Conference on Computing, Communication and Automation, ICCCA, 2017, pp. 350–354.

[65] Jiang, Lu, Learning intentional communication for multi-agent cooperation, in: Advances in Neural Information Processing Systems, 725, 2018, pp. 4–7264.

[66] Li Xiao, He Zhu, Liu, Song, Generating adversarial examples with adversarial networks, 2018b, ArXiv preprint arXiv:1801.02610.

[67] Li, Yuxi, Deep reinforcement learning: An overview, 2017, ArXiv preprint arXiv:1701.07274.

[68] Dan Li, Dacheng Chen, Jonathan Goh, See-kiong Ng, Anomaly detection with generative adversarial networks for multivariate time series, 2018a, ArXiv preprint arXiv:1809.04758.

[69] Moshe Kravchik, AsafShabtai, Detecting cyber attacks in industrial control systems using convolutional neural networks, in: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, 2018, pp. 72–83.

[70] Mamoru Mimura, Hidema Tanaka, Heavy log reader: learning the context of cyber attacks automatically with paragraph vector, in: International Conference on Information Systems Security, 2017, pp. 146–163.

[71] Alazab Vinayakumar, Poornachandran Soman, Venkatraman, Robust intelligent malware detection using deep learning, IEEE Access 7 (2019a) 46717–46738.

[72] D. Vasan, M. Alazab, S. Wassan, H. Naeem, B. Safaei, Q. Zheng, IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture, Comput. Netw. 171 (2020) 107138.

[73] MamounAlazab Vinayakumar, PrabaharanPoornachandran Soman, Ameer Al-Nemrat, SitalakshmiVenkatraman, IEEE Access 7 (2019b) 41525–41550, Vinayakumar.

[74] H.S. Chae, B.O. Jo, S.H. Choi, T.K. Park, Feature selection for intrusion detection using NSL-KDD, Recent Adv. Comput. Sci. 18 (2013) 4–187.

[75] M. Hatada, M. Akiyama, T. Matsuki, T. Kasama, Empowering anti-malware research in Japan by sharing the MWS datasets, J. Inf. Process. 23 (5) (2015) 579–588.

[76] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, K. Nakao, Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation, in: Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, 2011, pp. 29–36.

[77] N. Moustafa, J. Slay, UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), in: 2015 Military Communications and Information Systems Conference, MilCIS, IEEE, 2015, pp. 1–6.

[78] R. Panigrahi, S. Borah, A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems, Int. J. Eng. Technol. 7 (3) (2018) 479–482, 24.

[79] J. Yang, Y.Q. Shi, E.K. Wong, X. Kang, JPEG steganalysis based on densenet, 2017b, arXiv preprint arXiv:1711.09335.

[80] Andrade Meira, Carneiro Praca, Alonso-Betanzos Bolón-Canedo, Marreiros, Performance evaluation of unsupervised techniques in cyber-attack anomaly detection, J Amb. Intell. Huma. Comput. (2019) 1–13.

[81] Thing, Network anomaly detection and attack classification: A deep learning approah, in: IEEE Wireless Communications and Networking Conference, 2017, pp. 1–6.

[82] Carro Lopez-Martin, Sanchez-Esguevillas, Lloret, Sensors 17 (9) (2017) 1967.

[83] Bo Du, Wei Xiong, Jia Wu, Lefei Zhang, Stacked convolutional denoising auto-encoders for feature representation, IEEE Trans. Cybern. 47 (4) (2016) 1017–1027.

[84] Guifang Liu, HuaiqianBao, Baokun Han, A stacked auto encoder-based deep neural network for achieving gearbox fault diagnosis, Math. Probl. Eng. (2018).

[85] U.S.K.P.M. Thanthrige, J. Samarabandu, X. Wang, Machine learning techniques for intrusion detection on public dataset, in: 2016 IEEE Canadian Conference on Electrical and Computer Engineering, CCECE, IEEE, 2016, pp. 1–4.

[86] Florian Skopik, Giuseppe Settanni, Roman Fiedler, A problem shared is a problem halved: A survey on the dimensions of collective cyber defence through security information sharing, Comput. Secur. 60 (2016) 154–176.

[87] Huaizhi Wang, JiaqiRuan, Zhengwei Ma, Bin Zhou, Xueqian Fu, Guangzhong Ca, Deep learning aided interval state prediction for improving cyber security in energy internet, Energy 174 (2019) 1292–1304.

[88] Geethapriya Thamilarasu, ShivenChawla, Towards deep-learning-driven intrusion detection for the internet of things, Sensors 19 (1977) (2019).

[89] Khaled Alrawashdeh, Carla Purdy, Fast hardware assisted online learning using unsupervised deep learning structure for anomaly detection, in: 2018 International Conference on Information and Computer Technologies, 2018, pp.128-134.

[90] H. Zhang, Y. Li, Z. Lv, A.K. Sangaiah, T. Huang, A real-time and ubiquitous network attack detection based on deep belief network and support vector machine, IEEE/CAA J. Autom. Sin. 7 (3) (2020b) 790–799.

[91] Mahmoud Nabil, Muhammad Ismail, Mohamed Mahmoud, MostafaShahin, Khalid Qaraqe, ErchinSerpedin, Deep learning-based detection of electricity theft cyber-attacks in smart grid AMI networks, in: Deep Learning Applications for Cyber Security, 2019, pp. 73–102.

[92] Zachary Lipton, John Berkowitz, Charles Elkan, A critical review of recurrent neural networks for sequence learning, 2015, ArXiv preprint arXiv:1506.00019.

[93] Hazarika Young, Poria, Cambria, Recent trends in deep learning based natural language processing, IEEE Comput. Intell. Mag. 13 (3) (2018) 55–75.

[94] ThanhThi Nguyen, Vijay JanapaReddi, Deep reinforcement learning for cyber security, 2019, ArXiv preprint ArXiv:1906.05799.

[95] Sankar Salehinejad, Colak Barfett, Valaee, Recent advances in recurrent neural networks, 2017, ArXiv preprint arXiv:1801.01078.

[96] Alazab Venkatraman, Vinayakumar, A hybrid deep learning image-based analysis for effective malware detection, J. Inf. Secur. Appl. 47 (2019) (2019) 377–389.

[97] Elaine Raybourn, Michael Kunz, David Frit, Vince Urias, A zero-entry cyber range environment for future learning ecosystem, in: Cyber-Physical Systems Security, 2018, pp. 93–109.

[98] L.N. Darlow, E.J. Crowley, A. Antoniou, A.J. Storkey, CINIC-10 is not imagenet or CIFAR-10, 2018, arXiv preprint arXiv:1810.03505.

[99] Roychowdhury Allen, Liu, Reward-based Monte Carlo-Bayesian reinforcement learning for cyber preventive maintenance, Comput. Ind. Eng. 126 (2018) 578–594.

[100] Aidin Ferdowsi, Ursula Challita, WalidSaad, Narayan B. Mandalay, Robust deep reinforcement learning for security and safety in autonomous vehicle systems, in: IEEE International Conference on Intelligent Transportation Systems, ITSC, 2018, pp.307–312.

[101] Lantao Yu, Yi Wu, Rohit Singh, Lucas Joppa, Fei Fang, Deep reinforcement learning for green security game with online information, in: Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence, 2018.

[102] Zilong Lin, Yong Shi, ZhiXue, Idsgan: Generative adversarial networks for attack generation against intrusion detection, 2018, ArXiv preprint arXiv:1809.02077.

[103] Rajendran Balakrishnan, Pelusi, Ponnusamy, Deep belief network enhanced intrusion detection system to prevent security breach in the internet of things, Internet Things (2019) 100112.

[104] SujitRokka Chhetri, Anthony Bahadir Lopez, Jiang Wan, Mohammad Abdullah Al Faruque, GAN-Sec: Generative adversarial network modelling for the security analysis of cyber-physical production systems. IEEE: Automation and Test in Europe Conference and Exhibition, DATE, 2019, pp. 770–775.

[105] Chuanlong Yin, Yuefei Zhu, Shengli Liu, JinlongFei, He tong Zhang, An enhancing framework for bonnet detection using generative adversarial networks, in: 2018 International Conference on Artificial Intelligence and Big Data, 2018, pp 228–234.