JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Survey of Deep Learning Algorithms for Cyber Security Applications

[1]ASRA SARWATH, [2]Dr. RAAFIYA GULMEHER
[1]Research Scholar, [2]Assistant Professor
[1]Department of Computer Science and Engineering,
Faculty of Engineering and Technology,
[1]Khaja Bandanawaz University, Kalaburagi, Karnataka, India

Abstract: Cyber security primarily protects the hardware, software, and data in a system with an active internet connection from outside attacks. Organizations primarily use cyber security to protect their databases and systems from unauthorized access. These security issues are caused by various types of attacks such as phishing, spear-phishing, a drive-by attack, a password attack, denial of service, and so on. We analyzed and reviewed the use of deep learning algorithms for cyber security applications in this survey. Because data are so important in Deep Learning (DL) methods, we describe some of the most commonly used network datasets in DL, discuss the challenges of using DL for cyber security, and make recommendations for future research.

***IndexTerms* – cyber-attacks, cyber security applications, deep Learning, machine learning, open-source datasets, real-time datasets,**

I. Introduction

Cloud computing [1], big data [2], the Internet of Things, and the growth of software-based networks are all driving rapid growth in cyberspace. Cyber security is a common issue in cyberspace. Cyber security is a method of protecting systems, applications, and networks from cyber-attacks. The attackers' primary goal in carrying out these attacks is to modify/access confidential information, launder money from users, and disrupt normal business operations. The large number of devices connected to the network and the novel attacks carried out by hackers are the challenges associated with implementing cyber security policies on organizations. Tools such as intrusion detection systems, firewalls, scanners, and antivirus software, among others, are used to prevent various types of attacks. Devices connected to the network are frequently subjected to a variety of attacks. The internet allows networks to communicate with one another and allows hardware, intelligence, software, information, and data to be exchanged. As a result, computer networks are extremely vulnerable to malware and other cyber security threats. The attackers are skilled at tracing data from cyberspace [3]. The massive amount of data and confidential information is protected by cyber security, and any attacks are automatically reported to the entire organisation. Furthermore, data science concepts applied to cyber security are used to classify anomalous detection characteristics, event correlation, and pattern identification. Because of their limited battery power, mobility, and energy consumption, mobile devices cannot be protected by an Intrusion Detection System (IDS). With the help of machine learning algorithms, a protective shield can be built to safeguard applications using cyber security [4-8]. When processing large amounts of data and providing security, modern computer systems add computational complexity. This obstacle can be overcome by incorporating Artificial Intelligence (AI) techniques [9]. Artificial intelligence refers to the rapid development of computer-based research, methods, and applications to replicate human intelligence (AI). AI techniques can quickly identify malware in an application and take appropriate action. It is also used to process the massive amounts of data generated by users on a daily basis. To identify these attacks, machine learning (ML) with increased amounts of security detection software, encoding, and thread extraction characteristics are required [10]. However, the deep learning concept is more effective. Deep learning is one of the most powerful machine learning techniques enabled by AI, and this study focuses on it. Deep learning techniques can process a large amount of information in cyber security datasets efficiently while resisting attacks [11]. As a result, many researchers focused on cyber security issues using deep learning concepts [12].These researchers [13-20] proposed a thorough examination of existing cyber security applications using deep learning techniques. These studies were primarily conducted to encourage various researchers working in the same field to improve the security of various organizations vulnerable to various potential attacks. However, these articles did not cover the wide range of cyber security datasets used, as well as the flaws in these deep learning techniques. As a result, the primary goal of this work is to present a bibliometric analysis of the deep learning approach used for detecting potential cyber security threats. A comparative analysis is then performed to review the various attacks encountered, the various platforms used, datasets, and learning models developed by various researchers in the field of cyber security using Deep Learning. This survey also addresses existing research challenges, open issues, and future research directions.

II. DL ALGORITHMS FOR CYBER SECURITY

Machine learning is a technique in which the system is taught to distinguish between good and bad files. A machine must first be trained with a set of features extracted from benign and malicious samples. Deep learning is a subset of machine learning, also known as deep neural networks (DNNs) [3]. Deep learning is a type of modern ML that can take raw inputs and learn the optimal feature representation implicitly. In numerous long-standing supervised and unsupervised artificial intelligence tasks such as natural language processing (NLP), image processing, speech recognition, and many others [3], deep learning architectures have produced remarkable results. Optimization and parallel and distributed computing technologies have made it possible to train large amounts of data in recent years. The way the brain works serves as inspiration for deep learning. Particularly, deep learning architectures are able to adjust the meaning of the data whenever it encounters new data and comprehend the meaning of large amounts of data. As a result, it does not require assistance from domain experts to comprehend the significance of new input. By passing information to multiple hidden layers, deep learning can learn hierarchical feature representation, which is a benefit.

Deep learning architectures must be applied to cyber security to improve cyber-attack and malware detection rates [4-19]. Cyber security use cases for intrusion detection, traffic analysis, and Android malware detection are taken into consideration in this work. Both traditional machine learning algorithms and deep learning architectures are thoroughly evaluated in intrusion detection. Deep learning architectures are used for traffic analysis and Android malware detection. Compared to traditional machine learning algorithms, deep learning architectures have the added advantage of being able to analyze security artifacts' large amounts of data. The best parameters determine the best performance for both traditional machine learning algorithms and deep learning architectures, which are both parameterized. In recent days, finding the best parameters for deep learning has remained a significant challenge.

Table 1 Classification of DL based on the cyber security attacks

Deep Learning Algorithms for Cyber security					
Convolutional Neural Network (CNN)	Auto encoder (AE)	Deep Belief Network (DBN)	Recurrent Neural Network (RNN)	Generative Adversarial Network (GAN)	Deep Reinforcement Learning (DRL)
1. Single CNN 2. Multi-CNN 3. Variants of CNN 4. Acoustic model of CNN 5. Limited weight sharing of CNN 6. Cyber security applications using CNN	1. Stacked Auto Encoder (SAE) 2. Denoising Auto Encoder (DAE) 3. Variational Auto Encoder (VAE)	1. Deep Boltzmann Machine (DBM) 2. Restricted Boltzmann Machine (RBM) 3. Deep Restricted Boltzmann Machine (DRBM)	1. Bidirectional RNN (BRNN 2. Long Short Term Memory (LSTM) 3. Acoustic model of RNN (ACNN) 4. Gated Recurrent Unit (GRU).	1. Generative modelling (GM), 2. Discriminative modelling (DM)	1. Multi-task reinforcement (MTR) 2. Multi-agent reinforcement (MAR) 3. Asynchronous reinforcement (AR) 4. Q-learning Reinforcement (QR)

Table 1 depicts the classification of deep learning algorithms based on cyber security attacks. DL is a new area of study in machine learning. Its motivation is to build a neural network that mimics the human brain for analytical learning. It uses a mechanism similar to the human brain to interpret data such as images, sounds, and texts [79]. Hinton [80] proposed the concept of deep learning (DL) based on the deep belief network (DBN), in which an unsupervised greedy layer-by-layer training algorithm is proposed that provides hope for solving the deep structure optimization problem.

Then, a multi-layer automatic encoder's deep framework is suggested. Furthermore, LeCun et al. [81] proposed the first true multilayer structure learning algorithm that uses a space relative relationship to reduce the number of parameters to improve training performance. DL is a machine-learning method based on data learning characterization. An analysis, such as an image, can be expressed in a number of ways, such as as a vector of each pixel intensity value, or more abstractly as a series of edges, a region of a specific shape, or something similar. Utilizing specific representations makes it easier to learn tasks from examples. DL methods, like ML methods, include supervised and unsupervised learning. Different learning frameworks result in very different learning models. The advantage of DL is the use of unsupervised or semi-supervised feature learning and hierarchical feature extraction to efficiently replace features manually [82].

III. LITERATURE SURVEY

The cyber security system is employed to identify various types of attacks using the deep learning method, as mentioned in this survey. We chose a deep learning-based cyber security attack detection concept for this survey.

Kravchik et al. [21] used 1-Dimensional CNN to investigate the various types of cyber-attacks kept in Industrial Control Systems. Their suggested technique successfully identified 31 different types of cyber-attacks out of 36 in the dataset using convolutional and recurrent neural networks. They applied the Secure Water Treatment (SWaT) dataset to the GoogleTensorflow framework platform. However, this technique has poor interpretability and fails to detect the other five-types of cyber-attacks that are present.

Mimura et al [22] developed a generic detection method that is free of attack methods and feature vectors. The primary goal of this technique is to identify adversary communication from proxy server logs. With F-measure values of 0.98 and 0.99, it identifies two attacks: command and control traffic and an unfamiliar drive-by download attack.

Vinayakumar et al. [23] classified cyber-attacks into two levels: network and host. When designing the Intrusion Detection System, they concentrated on dynamic malicious attacks and large datasets (IDS). However, this technique had a high computational cost.

Vasan et al. [24] introduced an image-based malware classification CNN approach. This method can detect various types of malware and classify them based on their family. An augmentation technique is used to overcome the data variance challenge in this case. This method has a slightly higher run time overhead.

Li et al. [25] demonstrated an anti-steganalysis method based on CNN for detecting malware in images. They concentrated on the evolutionary algorithm attack based on the Least Significant Bi and the gradient-based attack. It demonstrates significant ways to undermine steganalysis and the neural network's weakness.

Meira et al. [26] have used unsupervised model of learning to identify unfamiliar attacks using anomaly-based intrusion detection systems. This technique outperforms and is suitable for IDS, but it has a high false positive rate. NSL-KDD datasets are utilized in the experiments, and Python software is employed for implementation.

Thing et al [27] concentrated on IEEE 802.11 security and identified novel threats and attacks conducted on it. They used an unsupervised Deep Learning Approach to identify and classify the anomalies. The AWID-CLS dataset was used, and the approach was implemented. Even though the classification performance is accurate, the computational cost is high.

Martin et al. [28] introduced an IDS system that uses a conditional variational autoencoder to detect malicious labels within the decoder layer. It is capable of producing effective feature reconstruction and producing better classification results. This approach, however, produced lower classification results. It's built into the OMNET platform with an STL-10 dataset.

Diro et al [29] recognised cyber-attacks occurring in the Internet of Things environment, with a concentrate on zero-day attacks. They used hidden patterns in the training data to distinguish between malicious and normal traffic. The experiments are carried out with JAVA software, and the detection process is centralised but not suitable for analysing large amounts of data.

Bo Du et al [30] has proposed auto-encoders with stacked convolutional denoising for feature representation The supervised technique improves classification outcomes but is not suitable for maximising other stages. The NSL-KDD dataset is executed using the Python platform.

Guifang Liu et al, A deep neural network (DNN) based on stacked auto-encoders for diagnosing gearbox faults. The author employed the unsupervised learning process. This approach seems to be more scalable and adaptable, but it is not suited to large-scale experiments. The effectiveness of their proposed concept is evaluated using gearbox datasets and executed in the C++ programming language.

Skopik et al [32] revealed that information sharing between two organisations must be secured to prevent any future network attacks. Although it provides secure sharing of information, it is expensive and can only be deployed in critical infrastructures.

H. Zhang, et al [33] has proposed a network attack detection system that is both real-time and ubiquitous, based on deep belief networks and support vector machines. They have investigated the DBNB and support Vector Machine powered network IDS system.

Balakrishnan et al [34] invented an Intelligent IDS based on DBN to combat critical cyber-attacks inside the IoT environment. The primary objective of this approach is to detect the adversary's activity within the network once they cross the border. When trained on the MNIST dataset, this framework can precisely identify the data injection attacks. This model, however, had a high computational cost and a low accuracy.

Thamilarasu et al [35] also recommended intelligent intrusion detection systems for IoT systems that use deep learning algorithms to detect malicious traffic. With a larger bandwidth, this technique is more efficient and feasible. NSL-KDD is the dataset used, and it is executed in MATLAB. The researcher used the NSL-KDD, MNIST, and Kyoto datasets for the unsupervised deep learning process and successfully predicted denial of service and overflow attacks. Despite the fact that this technique provides high accuracy, complex hardware implementation is required.

Nabil et al. [36] had to use a deep feed-forward neural network and a recurrent neural network to recognise consumers who review false electricity usage. This is most common in the Advanced Metering Infrastructure (AMI), and it is also referred to as an electricity theft cyber-attack. To detect contamination attacks, this approach is implemented in real-time detectors that use the Python platform.

Venkatraman et al [37] suggested a hybrid deep learning architecture for malware detection in images. The primary goal is to detect suspicious behaviour using the various hybrid architectures. For malware detection, the Malimg, VirusSign, and VirusShare datasets are used, and the procedure is implemented in both Java and Python. In this method, the outputs are frequently misclassified.

Z. Lipton et al[38] has carried the critical review on recurrent neural networks for sequence learning and employs a supervised model with parallel computation but few translation and encoding operations. For training, the C++ language programme is used in conjunction with the COCO dataset.

H.Young et al [39] has investigated on Recent trends in the DL based natural language processing. The unsupervised learning model with the SST dataset is implemented using JAVA software. This method includes a Better forward procedure and is difficult to apply to large amounts of data. Salehinejad et al. [95] proposed a supervised model using the BABL dataset and the OMNET platforms. It is the simplest and most adaptable method, but it takes more time during weight transfer.

V. Mnih et al [40] has proposed the deep reinforcement learning based on Asynchronous methods. They demonstrated an unsupervised learning process using the CIFAR-10 dataset and JAVA software. This method is appropriate for detecting asynchronous demon attacks using a slower training speed.

Allen et al. [41] suggested a Monte Carlo Bayesian Reinforcement learning method to shorten the median estimated learning time and also provide faster learning. The cost of system implementation is especially high per host, as is the cost of identifying current threats in the system. The dataset is made up of malicious emails, and the system is built on a LINUX platform.

Nguyen et al [42] conducted a review of the widely used Deep Reinforcement Learning (DRL) models for detecting cyber-attacks in the system. The DRL technique is commonly used to solve dynamic, intricate, and multidimensional security problems with limited communication.

Ferdowsi et al. [43] introduced a DRL algorithm for autonomous vehicles to safeguard it from the cyber–physical attacks. Between the adversary and the Autonomous vehicle, a game theory model is created. In this case, the adversary injects malicious data into the sensor of the autonomous vehicle, altering the optimal spacing and causing accidents. This system protects against such an attack by reducing the adversaries' spacing deviation.

Yu et al. [44] utilised DRL to combat real-time attacks such as illegal woodcutting, poaching, and overfishing. The attacker is identified by using the deep Q network and the real-time information obtained. Obtaining the illegal member's footprints yields real-time information.

Radford et al. [45] introduced a Deep CNN-GAN pair to identify the set of malicious images. The unsupervised learning models have a hierarchical representation with noises that occur throughout a denial attack. The CIFAR-10 datasets are implemented on the Matlab environment. It has a hierarchical representation with noises that occur during overlap.

Z. Katzir et al[46], has investigated the resilience of ML classifiers used in cyber security are being quantified. Malwr is a supervised learning model for malware detection using dynamic analysis and an up-to-date dataset. As a result, it provides empirical and classified evidence but is unsuitable for a variety of tasks. Using this method, the partitioned attack is effectively detected.

Lin et al. [47] proposed an IDS-based GAN network that can generate adversarial attacks in order to compromise the IDS. The attack was a type of black-box attack. NSL-KDD is the dataset used, and it is executed on the LINUX platform. This technique is extremely resistant to various types of attacks and has a high computational complexity.

Chhetri et al. [48] proposed a GAN security model to combat cross-domain attacks in the cyber-physical framework. Complex security identification ensures maximum availability and integrity performance. The most common large-scale attacks that harms cyber security is the botnet attack.

Yin et al. [49] introduced a Botnet-based GAN (bot-GAN) to detect new botnets and overcome malicious attacks. The process is scalable and improves botnet detection, but it never takes into account payload information. The ISCX Botnet dataset is being used, and the framework is built with JAVA software.

IV. Cyber security Datasets

Currently, data is collected by various research groups for their own analysis as well as for distribution to community repositories [50]. Existing datasets have flaws such as outdated data, redundant information, and an unbalanced number of categories. Although the data can be improved after processing, there is a problem with insufficient data volume. As a result, establishing network intrusion detection datasets with large amounts of data, broad-type coverage, and balanced sample numbers of attack categories becomes a top priority in the field of intrusion. Machine learning/DL and artificial intelligence research are used to explain the following security-related datasets.

- ***KDD Cup 1999 Dataset:*** The data collected from MIT Lincoln Labs includes BSM list files, tcpdump, and KDD Cup 1999 [50]. This dataset includes data from the DARPA'98 IDS evaluation programme [51]. This dataset is also used as benchmark data for assessing intrusion detection systems. KDD'99 [50] is one of the well-known data sets for evaluating the performance of anomaly detection methods. Various researchers are currently using the KDD dataset [52, 53-55].
- ***NSL-KDD**:* NSL-KDD is an advanced form of the KDD-Cup-99 challenge data set provided by [56]. One method was to completely remove KDD-duplicate Cup-99's connection records in order to protect the classifier from a biassed state during training. Furthermore, the invalid records 136,489 and 136,497 were removed. The second step was to choose various types of connection records in order to effectively detect attacks during testing. The third attempted to reduce the rate of false detection by balancing the number of connection records between training and testing.This was still an effective data set for detecting misuse or anomalies. The data set, while not suitable for real-time network intrusion detection, can be used to effectively benchmark the newly introduced classifiers. The NSL-KDD data set[57] is superior to the KDD-Cup-99 data set, and it contains more 'DoS,' 'normal,' 'Probe,' and 'R2L' connection records. As a result, the machine learning classifier prioritises these data [58].
- ***ISOT (Information Security and Object Technology) Dataset:*** The ISOT dataset is composed of openly available botnets and normal datasets totaling 1,675,424 total traffic flows. The malicious traffic in ISOT was obtained from the French chapter of the honeynet project, which included the Storm and Waledac botnets [50, 59, 60, 61].
- ***HTTP CSIC 2010 Dataset:*** Large number of web requests generated automatically and developed at the Information Security Institute of CSIC (Spanish Research National Council) is referred to as the HTTP CSIC 2010 dataset [50]. This dataset can be used to test web attack protection systems. The above data is composed of nearly 6,000 normal requests and over 25,000 anomalous requests. Furthermore, HTTP requests are classified as abnormal or normal [50]. This dataset is used to successfully detect web pages in [62-64].
- ***CTU-13 (Czech Technical University) Dataset:*** The CTU-13 (Czech Technical University) dataset is a collection of 13 different malware seizures in a nonfictional network environment. The goal of this dataset is to collect real mixed botnet traffic. Keeping the preceding in mind, normal traffic is generated by verified normal hosts, whereas botnet traffic is generated by infected hosts [50]. One of the advantages of using this dataset is that it is a carefully labelled dataset that captures procedures performed in a controlled environment [65, 66, 67, 68].
- ***UNSW-NB15 Dataset:*** The UNSW-NB15 Dataset was reportedly generated by the IXIA Perfect Storm tool in the Australian Centre for Cyber Security's (ACCS) Cyber Range Lab [50]. This dataset contains nearly an hour of anonymized traffic traces from a DDoS attack in 2007 [69, 70-75]. Fuzzers, Backdoors, Analysis, Exploits, DoS, Reconnaissance, Generic, Worms, and Shellcode are included in this dataset [50].
- ***ADFA DATASET:*** The ADFA data set is a collection of data sets from the Australian Defence Academy (ADFA) [76] that are widely used in the testing of intrusion detection products. Various system calls in the dataset have been characterised and labelled for the type of attack. The data set contains two operating systems, Linux (ADFA-LD) and Windows (ADFA-WD) that also record the order of system calls. In the case of ADFA-LD, it keeps a record of the operating system's invocation for a set period of time.

Drawbacks of KDD-Cup-99

A detailed report on the major shortcomings of the KDD-Cup-99 challenge data is provided in [56]. The most common and well-known issue raised by many authors is that the data set does not accurately represent real-world network traffic. Despite harsh criticism, KDD-Cup-99 is used in many research studies to understand and know the effectiveness of various machine learning classifiers. Tavallaee et al. [56] performed a detailed analysis of tcpdump data and reported non-uniformity and simulated artefacts in the KDD-Cup-99 challenge data set.They tried to enhance the network anomaly detection performance using the KDD-Cup-99 and mixed KDD-Cup-99. They discovered that network attributes such as remote client address, TTL, TCP options, and TCP window are extremely small in KDDCup- 99 data compared to real-world network traffic data. Because KDD-Cup-99 is a subset of KDD-Cup-98, it continues to suffer from the exact same issues as KDD-Cup-98.

Tavallaee et al.'s report [56] have briefly discussed the low frequency of attacks as the reason for the decreased performance when attacking network connections; U2R and R2L categories. They reported the factors that contributed to their superior performance in classifying attacks into either the "R2L" or "U2R" categories.

However, a higher detection rate may be achieved by incorporating a few connection records belonging to the "R2L" and "U2R" categories into the existing KDD-Cup-99. However, they remained as a statement because they were unable to demonstrate the performance of the machine learning classifier on mixed data through experiments. The "snmpgetattack" that was reported in [56] shares similarities with attacks against "R2L" and normal connection records. As a result, the machine learning classifier fails to correctly classify the "snmpgetattack" category into the normal and "R2L" categories.

DARPA/KDD-Cup-98 initially failed to demonstrate the performance of classical IDS. Brugger and Chow [77] used DARPA/KDD-Cup-99 tcpdump traces as input data to evaluate Snort IDS's performance to address this issue. The framework brings about an extremely terrible showing for the assaults has a place with 'DoS' and 'Test' classification, predominantly because of the framework have taken on the decent signature sets as an instrument. The Snort system has demonstrated excellent performance in the "R2L" and "U2R" attacks categories, in contrast to high frequency attacks like "DoS" and "Probe"[78].

However many issues exists in KDD-Cup-99 test dataset, still generally been utilized for benchmarking the different AI classifier to arrange ID. Researchers [56] introduced NSL-KDD, a more refined version of the KDDCup-99 data set, to address the inherent issue. They constructed NSL-KDD by completely eliminating the connection records in indexes 136,489 and 136,498, as well as the redundant records in the train and test connection records. This prevents the classifier from being biased against connection records that appear frequently. Microsoft, Malimg, and various open-source datasets must be utilized. Due to privacy concerns in network traffic, there is very little open source data available for evaluating the effectiveness of various machine learning classifiers for N-IDS (network-based intrusion detection system). We must use the DARPA/KDD-Cup-99 challenge, a refined version of the KDD-Cup-99 challenge, as a benchmark for the effectiveness of deep learning algorithms; NSLKDD and the most recent data set of intrusions; UNSWNB-15

V. CYBER SECURITY CHALLENGES

Cyberspace has become an essential component of all aspects of modern life. The world's daily lives are becoming increasingly dependent on the internet. The risk of malicious threats has also increased as a result of the growing reliance on the internet. Cyber security has become the most important aspect of the cyber world in the fight against all cyber threats, attacks, and frauds because of the growing risks to cyber security. The expanding cyberspace is very vulnerable to the ever-increasing possibility of being attacked by cyber threats that never end. Cyber security is now the most important part of the country's overall strategies for economic and national security. In India, there are such countless difficulties connected with network protection. With the increment of the digital assaults, each association needs a security investigator who ensures that their framework is gotten. These security analysts face numerous cyber-security challenges, such as protecting private organization servers and government organizations' confidential data. The following is a list of recent significant challenges affecting cyber security:

- *Ransomware Evolution*

Ransomware is a kind of malware that locks the data on a victim's computer and demands payment before the ransomed data is unlocked. The victim's access rights were restored after a successful payment. Ransomware is the bane of cyber-security professionals, data professionals, IT professionals, and executives. Ransomware attacks are becoming more common in cybercrime. To protect their organisation, IT professionals and business leaders must have a strong recovery strategy against malware attacks. It entails careful planning to recover corporate and customer data and applications, as well as reporting any breaches in accordance with the Notifiable Data Breaches scheme. Today's DRaaS solutions offer the best protection against ransomware attacks. We can use DRaaS solutions to automatically backup our files, easily identify which backup is clean, and initiate a fail-over with the click of a button when malicious attacks corrupt our data.

- *Blockchain Revolution*

The most significant innovation in the modern era of computing is blockchain technology. We now have a truly native digital medium for peer-to-peer value exchange for the first time in human history. Cryptocurrencies like Bitcoin are made possible by a technology called the blockchain. The blockchain is a vast global platform that lets two or more people do business or conduct transactions without having to trust a third party. The cyber-security benefits that blockchain would provide are difficult to predict. Blockchain is something that cyber security experts can educated guess about. As blockchain's application and utility in digital protection arise, there will be a sound strain, however there will likewise be reciprocal mixes with laid out, customary network safety techniques.

- *Internet of Things Threats*

An interconnected network of physical devices that can be accessed via the internet is known as the Internet of Things (IoT). The physical devices that are connected have a unique identifier (UID) and can transfer data over a network without the need for human-to-human or computer-to-computer interaction. Consumers and businesses are particularly vulnerable to cyberattacks due to the firmware and software running on IoT devices.

When IoT devices were designed, their commercial and cyber-security applications were not taken into account. So every association needs to work with network protection experts to guarantee the security of their secret key strategies, meeting taking care of, client confirmation, multifaceted validation, and security conventions to help in dealing with the risk.

- *Artificial intelligence Expansion*

John McCarthy, the inventor of artificial intelligence, defined AI as " Making intelligent machines, particularly intelligent computer programs, is a field of science and engineering. The development of intelligent machines that function and behave like humans is the focus of this subfield of computer science. Speech recognition, learning, planning, problem-solving, and other related activities are among them. Our cyber-security strategy greatly benefits from AI's ability to mitigate the impact of an attack by protecting and defending an environment as soon as it begins. When a threat has an impact on a business, AI takes immediate action to defend against it. IT business pioneers and network safety technique groups consider man-made intelligence as a future defensive control that will permit our business to remain in front of the digital protection innovation bend.

- *Server less Apps Vulnerability*

An application that relies on third-party cloud infrastructure or a back-end service like Google Cloud Function or Amazon Web Services (AWS) Lambda, among others, is known as server less architecture and apps. Because users access the application locally or off-server on their device, server-less applications make it easier for cyber attackers to spread threats on their system. As a result, when using a server-less application, it is up to the user to take security precautions. Our data is still accessible to the attackers despite the servers' absence of apps. The server-less application is useless if an attacker exploits a vulnerability, such as a compromised insider or leaked credentials, to gain access to our data. We can use the application that gives us the best chance of defeating cybercriminals to run software. The server less applications are normally little in size. It makes it easier and faster for developers to launch their applications. They need not be concerned about the infrastructure underneath. Server-less applications include, but are not limited to, web services and data processing tools.

VI. OPEN ISSUES AND FUTURE RESEARCH DIRECTION

Based on previous research, it is clear that an effective deep learning method for security attack detection has been investigated and designed. Each performance result, such as accuracy, precision, recall, sensitivity, specificity, and acuteness, is best and widely accepted; however, it contains a few complications due to their method, platform, algorithms, and so on. So many studies have been conducted in order to successfully resolve these issues, and a few of the research gaps and future work identified are as follows.

- According to the literature, no research has been conducted on the detection and classification of network intrusions based on the type of attacks used and the classes to which they belong.

  Future work: There is a need for research into intrusion detection and classification, as well as the types and classes of attacks. In addition, DL techniques must be tested against a variety of other cyber-security threats.
- It is also clear that the deep learning methodology designed to solve cyber security problems is solely focused on malware detection. To identify a broad range of attack vectors, the deep learning model should be combined with multiple machine learning methodologies and encryption algorithms.

  Future work: To improve performance, multiple deep learning models may be employed in parallel. Researchers should also concentrate on issues such as how an attacker uses the Deep Learning technique to gain access to a victim's system that is already secured with deep learning techniques.
- Moreover, researchers are publishing the results of their performance evaluations of their proposed models using various metrics. Some publish the recall, while others only focus on accuracy. There should be standardised metrics for comparing model performance. Most researchers have only published the accuracy of their model, leaving out other metrics. False-negative is a value that describes the situation in which an unauthorised user has been granted access to a system and network. Rather than considering accuracy, this would have a significantly negative impact on system performance.

  Future work: There must be standard metrics in place to compare models using various measurements. This could then be a watershed moment for future research to improve model performance.

  Furthermore, it has been discovered that the normal data-to-malware ratio used in the training dataset frequently deters performance. To assess the efficiency of the created cyber-security application, performance metrics such as speed, suspension of data poisoning, storage consumption, True Positive Rate, and False Positive Rate should be examined.
- We have also observed that, even in 2020, researchers are applying and testing the most recent machine learning and deep learning techniques on datasets that are more than 15 years old, such as the DARPA and KDD Cup datasets. However, we have observed a scarcity of cutting-edge datasets for spam and malware detection problems. On their customised datasets, researchers are employing cutting-edge machine learning techniques. They claim to have better model accuracy without disclosing their datasets or code used to generate the results. Customized datasets are frequently collected in a specific manner with little diversity, and their proposed model(s) performed well on those datasets. When the same models are tested on another similar problem domain on a different dataset, the models do not produce the same best results as claimed by the authors on their customised datasets. Obtaining a real malware dataset in real time is a difficult and time-consuming task. Until now, all research has been done on the malware dataset through experimentation or reverse engineering of the virus.

  Future work: As a result, future research can concentrate on experimenting with various open-source datasets and benchmark models. More research is needed to evaluate the performance of deep learning models using the most recent, benchmark, and real-time datasets.
- Also, the deep learning technique associated with cyber-security has a higher cost complexity associated with it during error solving. Because deep learning techniques are similar to black boxes, determining the root cause of an error is extremely difficult.

  Future work: In the future, the underlying causes of attacks should be thoroughly investigated in order to develop an active learning approach for cyber-security applications.
- The resource's basic requirements are high performance, GPU, larger storage, a low false-positive rate, and accurate information. It is also evident that the algorithms investigated and designed for larger resources are not highly scalable, have high power consumption, and are not flexible. The majority of the designs have a high computational cost, are difficult to implement, and have a complicated hyper parametric structure.

Future work: In future there need to design a highly scalable, low power consumption and flexible algorithm for larger resources.

Based on the research gaps identified above, it is clear that effective DL algorithms must be investigated and designed in order to solve the aforementioned issues and design a robust cyber-security application. The performances of DL models need to be evaluated with benchmark datasets, open-source datasets and real-time datasets.

VII. Conclusion

The use of deep learning in cyber security attacks is successfully discussed. We also provided a thorough examination of the documented applications of DL methods to detect these cyber-attacks. As a result, benchmark datasets are essential for advancing DL in the cyber security domain. The example papers that explain various DL techniques in the cyber domain were carefully selected, and widespread classes of various datasets were defined, along with their benefits and drawbacks.

As such, the purpose of this survey is to provide a useful body of work that will encourage researchers to advance the state of DL for cyber security systems.

In the future, we intend to introduce an efficient algorithm to address open issues and design a robust cyber security application. We identified future research opportunities related to developing new datasets to motivate work in developing new DL approaches for cyber security, as well as the need for approaches to be developed that consider the adversary's ability to use DL as a tool to subvert DL detection mechanisms.

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 selfadaptive 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 crossoverbased 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, Cyberphysical 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. 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] 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.

[22] M. Mimura, H.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.

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

[24] 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.

[25] 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.

[26] 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.

[27] Thing, Network anomaly detection and attack classification: A deep learning approach, in: IEEE Wireless Communications and Networking Conference, 2017, pp. 1–6.
[28] Carro Lopez-Martin, Sanchez-Esguevillas, Lloret, Sensors 17 (9) (2017) 1967.
[29] Diro, Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Gener. Comput. Syst. 82 (2018) 761–768.
[30] Bo Du, Wei Xiong, Jia Wu, Lefei Zhang, Stacked convolutional denoising auto-encoders for feature representation, IEEE Trans. Cybern. 47 (4) (2016) 1017–1027.
[31] Guifang Liu, HuaiqianBao, Baokun Han, A stacked auto encoder-based deep neural network for achieving gearbox fault diagnosis, Math. Probl. Eng. (2018).
[32] 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
[33] 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.
[34] Rajendran Balakrishnan, Pelusi, Ponnusamy, Deep belief network enhanced intrusion detection system to prevent security breach in the internet of things, Internet Things (2019) 100112
[35] G. Thamilarasu, S. Chawla, Towards deep-learning-driven intrusion detection for the IoT, Sensors 19 (1977) (2019).
[36] M. Nabil, M. Ismail, M. Mahmoud, MostafaShahin, K. Qaraqe, E. Serpedin, 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.
[37] Alazab Venkatraman, Vinayakumar, A hybrid deep learning image-based analysis for effective malware detection, J. Inf. Secur. Appl. 47 (2019) (2019) 377–389.
[38] Z. Lipton, J. Berkowitz, C. Elkan, A critical review of recurrent neural networks for sequence learning, 2015, ArXiv preprint arXiv:1506.00019.
[39] H.Young, Poria, Cambria, Recent trends in deep learning based natural language processing, IEEE Comput. Intell. Mag. 13 (3) (2018) 55–75
[40] V. Mnih, AdriaPuigdomenechBadia, M. Mirza, A. Graves, T. Lillicrap, T.Harley, D. Silver, K. Kavukcuoglu, Asynchronous methods for deep reinforcement learning, in: International Conference on Machine Learning, 2016, pp. 1928–1937.
[41] Roychowdhury Allen, Liu, Reward-based Monte Carlo-Bayesian reinforcement learning for cyber preventive maintenance, Comput. Ind. Eng. 126 (2018) 578–594.
[42] T. Nguyen, Vijay JanapaReddi, Deep reinforcement learning for cyber security, 2019, ArXiv preprint ArXiv:1906.05799.
[43] A. Ferdowsi, U. 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.
[44] 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.
[45] Alec Radford, Luke Metz, SoumithChintala, Unsupervised representation learning with deep convolutional generative adversarial network, 2015, ArXiv preprint arXiv:1511.06434
[46] Z. Katzir, Y. Elovici, Quantifying the resilience of machine learning classifiers used for cyber security, Expert Syst. Appl. 92 (2018) 419–429.
[47] Zilong Lin, Yong Shi, ZhiXue, Idsgan: Generative adversarial networks for attack generation against intrusion detection, 2018, ArXiv preprint arXiv:1809.02077.
[48] S. Chhetri, A. B Lopez, J. Wan, Mohammad A. Al Faruque, GAN-Sec: Generative adversarial network modeling for the security analysis of cyber-physical production systems. IEEE: Automation and Test in Europe Conference and Exhibition, DATE, 2019, pp. 770–775.
[49] Chuanlong Yin, Yuefei Zhu, Shengli Liu, JinlongFei, He tong Zhang, Anenhancing framework for bonnet detection using generative adversarial networks, in: 2018 International Conference on Artificial Intelligence and Big Data, 2018, pp 228–234.
[50] Yavanoglu, O., Aydos, M.: A review on cyber security datasets for machine learning algorithms. In: 2017 IEEE International Conference on Big Data (Big Data), pp. 2186–2193 (2017)
[51] Fraley, J.B., Cannady, J.: The promise of machine learning in cybersecurity. SoutheastCon 2017, 1–6 (2017)
[52] Xie, M., Hu, J., Slay, J.: Evaluating host-based anomaly detection systems: application of the one-class SVM algorithm to ADFA-LD. In: 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 978–982 (2014)
[53] Chowdhury, S., et al.: Botnet detection using graph-based feature clustering. J. Big Data 4 (1), 14 (2017)
[54] Neethu, B.: Adaptive intrusion detection using machine learning. Int. J. Comput. Sci. Netw. Secur. 13(3), 118 (2013)
[55] Kozik, R., Choraś, M., Renk, R., Hołubowicz, W.: A proposal of algorithm for web applications cyber attack detection. In: IFIP International Conference on Computer Information Systems and Industrial Management, pp. 680–687 (2015)
[56] M. Tavallaee, E. Bagheri,W. Lu, and A. A. Ghorbani, ``A detailed analysis of the KDD CUP 99 data set,'' in Proc. IEEE Int. Conf. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 1_6.
[57] G. Meena and R. R. Choudhary, ``A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA,'' in Proc. Int. Conf. Comput., Commun. Electron., 2017, pp. 553_558.
[58] Javaid, A., Niyaz, Q., Sun, W., Alam, M.: A deep learning approach for network intrusion detection system. In: Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 21–26 (2016)
[59] Bhamare, D., Salman, T., Samaka, M., Erbad, A., Jain, R.: Feasibility of supervised machine learning for cloud security. In: 2016 International Conference on Information Science and Security (ICISS), pp. 1–5 (2016)
[60] Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. Comput. Netw. 34(4), 579–595 (2000)
[61] Saad, S., et al.: Detecting P2P botnets through network behavior analysis and machine learning. In: 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 174–180 (2011)
[62] B. Alom, Taha, Intrusion detection using deep belief networks, , NAECON, 2015, pp. 339-344.
[63] Ugo Fiore, Francesco Palmieri, Network anomaly detection with the restricted Boltzmann machine, Neurocomputing 122 (3) (2014) 13–23.

[64] 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.
[65] Kato, K., Klyuev, V.: An intelligent DDoS attack detection system using packet analysis and support vector machine. In: IJICR, pp. 478–485 (2014)
[66] Yusof, A.R., Udzir, N.I., Selamat, A.: An evaluation on KNN-SVM algorithm for detection and prediction of DDoS attack. In: International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, pp. 95–102 (2016)
[67] Saad, S., et al.: Detecting P2P botnets through network behavior analysis and machine learning. In: 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 174–180 (2011)
[68] Hoque, N., Bhattacharyya, D.K., Kalita, J.K.: A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. In: 2016 8th International Conference on Communication Systems and Networks, pp. 1–2 (2016)
[69] T. Giménez, C., P. Villegas, A., A. Maranón, G.: An anomaly-based approach for intrusion detection in web traffic (2010)
[70] Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. Comput. Netw. 34(4), 579–595 (2000)
[71] T. Gimenez, C., P. Villegas, A., Alvarez, G.: A self-learning anomaly-based web application firewall. In: Computational Intelligence in Security for Information Systems, pp. 85–92. Springer (2009)
[72] 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.
[73] 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.
[74] 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.
[75] 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.
[76] M. Xie, J. Hu, X. Yu, and E. Chang, ``Evaluating host-based anomaly detection systems: Application of the frequency-based algorithms to ADFA-LD,'' in Proc. Int. Conf. Netw. Syst. Secur., 2014, pp. 542_549
[77]. Brugger S, Chow J (2005) An assessment of the DARPA IDS evaluation dataset using snort. Tech. Rep. CSE-2007-1, Department of Computer Science, University of California, Davis (UCDAVIS)
[78] R. P. Lippmann et al., ``Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation,'' in Proc. DARPA Inf. Survivability Conf. Expo. (DISCEX), vol. 2, 2000, pp. 12_26.
[79] Y. LeCun, Y. Bengio, and G. Hinton, ``Deep learning,'' Nature, vol. 521, pp. 436_444, May 2015.
[80] G. E. Hinton, ``Deep belief networks,'' Scholarpedia, vol. 4, no. 5, p. 5947, 2009.
[81] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, ``Gradient-based learning applied to document recognition,'' Proc. IEEE, vol. 86, no. 11, pp. 2278_2324, Nov. 1998.
[82] L. Deng and D. Yu, ``Deep learning: Methods and applications,'' Found. Trends Signal Process., vol. 7, nos. 3_4, pp. 197_387, Jun. 2014.