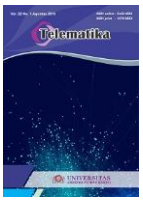

Available online at :
http://ejournal.amikompurwokerto.ac.id/index.php/telematika/

Telematika

Accreditated SINTA "2" Kemenristek/BRIN, No. 85/M/KPT/2020

Survey on Deep Learning Based Intrusion Detection System

Omar Muhammad Altoumi Alsyaibani[1], Ema Utami[2], Anggit Dwi Hartanto[3]

[1,2,3] Department Master Of Informatics, Universitas AMIKOM Yogyakarta
E-mail: omar.muhammad.aa@gmail.com[1], ema.u@amikom.ac.id[2], anggit@amikom.ac.id[3]

ARTICLE INFO

History of the article:
Received June 12, 2021
Revised July 16, 2021
Accepted August 26, 2021
Available online August 31, 2021

Keywords:
Deep Learning,
IDS Research,
IDS Review,
Deep Learning Model,
IDS Dataset

Correspondece:
Telepon: +62823 24254498
E-mail:
omar.muhammad.aa@gmail.com

ABSTRACT

Development of computer network has changed human lives in many ways. Currently, everyone is connected to each other from everywhere. Information can be accessed easily. This massive development has to be followed by good security system. Intrusion Detection System is important device in network security which capable of monitoring hardware and software in computer network. Many researchers have developed Intrusion Detection System continuously and have faced many challenges, for instance: low detection of accuracy, emergence of new types malicious traffic and error detection rate. Researchers have tried to overcome these problems in many ways, one of them is using Deep Learning which is a branch of Machine Learning for developing Intrusion Detection System and it will be discussed in this paper. Machine Learning itself is a branch of Artificial Intelligence which is growing rapidly in the moment. Several researches have showed that Machine Learning and Deep Learning provide very promising results for developing Intrusion Detection System. This paper will present an overview about Intrusion Detection System in general, Deep Learning model which is often used by researchers, available datasets and challenges which will be faced ahead by researchers.

INTRODUCTION

Network security is one of important areas in network implementation, particularly in a network which serves important service or contain important or crucial data. Network security has become research area for a long time for many organizations and scientist who conduct research in network development. As the network develops rapidly, issues related to network security also begin to vary. Based on data (CyberEdge Group, 2020) it is known that attacks on enterprise networks have increased in the last five years. Some of these attacks are ransomware attacks, malware, denial of service (DoS) and advanced persistent threats.

The purpose of various attacks is generally to obtain, destroy, obscure or alter information. There are many forms of network security implementation ranging from AAA systems (Authentication, Authorization & Accounting), Firewalls, Routing Filters, Access Control, Intrusion Prevention Systems, Intrusion Detection Systems, Honeypot, and others. This paper will focus on the Intrusion Detection System.

According to (Bace & Mell, 2001) intrusion detection is a technique of monitoring activities and events which occur on a computer system or network and analyzing it for signs of interruption. In recent years with the increasing computing speed, artificial intelligence has begun to develop rapidly, especially in the field of Machine Learning. Many studies can be found in many journals regarding the implementation

of Machine Learning-based IDS with various datasets used. Deep Learning, which is a branch of Machine Learning, has also begun to be widely used to implement IDS. Many researchers are interested in it because of the deep learning algorithm that which to act like the way human think. This paper will review essential matters related to research in the development of IDS based on deep learning.

Several studies have been done in reviewing deep learning-based IDS. For instance, research (Berman et al., 2019) which described deep learning methods used in cyber security, performance metrics of deep learning, application of deep learning based IDS, and portray studies in this area. Study (Ring et al., 2019) focused on depicting dataset for network-based intrusion detection system. It represents a complete point of view for IDS dataset. The same work also was done by authors (Hindy et al., 2020). This study also researched on dataset for intrusion detection.

Authors (Drewek-Ossowicka et al., 2021) characterized usage of neural network only for intrusion detection system. Yet in the study, the author narrated the deep learning methods, public datasets for IDS, and result of several previous studies. Study (Gamage & Samarabandu, 2020) described the datasets and deep learning models, compared and calculated both of them. Authors (Aldweesh et al., 2020) wrote a long paper about deep learning approach for deploying anomaly-based intrusion detection system. In detail, this work presents deep learning models, comparison between deep learning and shallow model, the datasets and comparison of several previous researches in this area.

This study will cover the deep learning models, datasets, frameworks, recent studies and research challenge in this area.

RESEARCH METHODS

This review paper begins with a brief literature review to see a general overview of the Deep Learning-based Intrusion Detection Systems topic. After getting a general information, authors then prepare the paper structure. This was followed by raising several questions related to IDS based on Deep Learning. Because this paper aims to help readers understand this topic from the ground up, especially readers who are still unfamiliar with IDS and Deep Learning, the questions which were raised also start from the basics.

Q1: What are the types / categories of IDS?

Q2: What are models/algorithms that exist in Deep Learning?

Q3: Which datasets are possible to use?

Q4: What framework can be used?

Q5: What researches has been conducted?

Q6: What are the research challenges in the future?

After the above questions were formed, the next step was to do the paper review itself. The search for research papers to answer Q4 was done using keywords “intrusion detection” or “intrusion detection system” and “deep learning” ((intrusion detection OR intrusion detection system) AND deep learning). In addition, paper selection is limited to papers published no later than 2016. Google Scholar as a good paper search engine as well as a tool for indexing papers, was used as the main tool for conducting paper searches and also as a benchmark for recording the number of citations for each paper. After the required papers have been collected, the information contained in each paper is organized and compiled to answer the seven questions above. The final step in the process of this paper review is to write the search results into the paper.

RESULTS AND DISCUSSION

1. Intrusion Detection System

Intrusion Detection System was initiated by (Anderson, 1980) in 1980. Various IDS products were created in 4 decades of IDS development. During its development, there were various kinds of problems that arose, for instance, the high rate of false alarms which is sending alerts when there was no dangerous traffic. This will increase the network security analyst workload. If the network security analyst keeps getting false alarm alerts, then it is possible that the actual attack is infiltrate into one of these false alarms. Therefore, many studies on IDS focus on reducing the number of false alarms and increasing the ability to detect malicious traffic. On the other hand, traditional IDS is incapable of detecting unrecognized attacks. Changes in conditions and the network environment are very fast and the emergence of various new technologies on the network also raises various types of new attacks. Therefore, it is urgent to develop an IDS that can detect attacks that are not even recognized (unknown attack).

To address the problem above, many researchers have started using Machine Learning as a method for developing intrusion detection systems. Machine Learning is an artificial intelligence technique which is able to dig and discover valuable information from a huge dataset (Fulkerson et al., 1995). An IDS based on Machine Learning can be a good IDS with a high level of detection accuracy if sufficient datasets are available and Machine Learning models are created using the right method. Machine Learning is easy for many people to learn because it does not depend on one field of science. Furthermore, Deep Learning has better performance compared to Machine Learning methods in processing bigdata. The difference in characteristics between Machine Learning and Deep Learning is how they do calculations. Deep Learning will create several hidden layers in its processing. Meanwhile, traditional Machine Learning models only have 1 processing layer. Therefore, the traditional machine learning model is often termed as shallow model.

Generally, IDS can be classified based on the detection method into two types, Anomaly-based IDS and Misuse / Signature-based IDS (Aghdam & Kabiri, 2016). Anomaly-based IDS will perform detection by comparing a traffic with normal traffic beforehand. If a traffic looks different than usual traffic, it will be detected as an anomaly traffic. Then, IDS will send a warning alert to the network administrator. On the other hand, Signature-based IDS will compare each traffic with the attack signature database which has been prepared on the IDS. If a traffic is similar to one or more signature database entries, then IDS will send alerts to the administrator. The advantages of Signature-based IDS are the low false alarms and provide detail reports. If a malicious traffic pattern does not exist in the IDS database, then IDS cannot detect it and IDS will not report anything to the administrator. Moreover, this type of IDS also cannot detect new type or pattern of malicious traffic so that administrators must keep IDS database update. Anomaly-based IDS attempts to deal with this weakness. The most important thing in preparing Anomaly-based IDS is to define a normal traffic database in detail and as many as possible, so that Anomaly-based IDS will be able to recognize anomalous traffic patterns. If various new protocols and services traffic appears on the network which are not in the IDS database, this will raise a false alarm. In addition, this type of IDS cannot provide accurate and detailed reports to administrators because it only contains a normal traffic database.

Based on the data source, IDS can also be classified into two types, Host-based IDS and Network-based IDS (Heberlein et al., 1989). Host-based IDS is implemented on a specific host and

focuses on detecting malicious traffic entering that host. This type of IDS can detect in detail because it can monitor any suspicious activity on the system either in files, programs and ports. On the other hand, Network-based IDS is placed on a network device or on a host which can access every activity on the network. This type of IDS focuses on checking every activity on the network, usually by considering traffic addresses in network communication. In Network-based IDS, data is usually divided into 3, namely packet data, data flow and session data. Host-based IDS will get its data source by accessing logs.

2. Deep Learning Model

a. Restricted Boltzman Machine (RBM)

The RBM model consists of hidden layers and visible layers. Units which are on the same layer are not connected to each other and follow the rules of the Boltzmann Distribution. Each neuron stores the weight computation which occur in every layer. Using randomly generated stochastic coefficients, input weights can be sent by nodes in a random process (Alrawashdeh & Purdy, 2017). RBM does not differentiate between forward and backward direction because it assumes the same weight of both. RBM is an unsupervised learning model that is trained by a contrastive divergence algorithm (Deng et al., 2013) and is usually used to perform feature extraction and denoising.

b. Deep Belief Network (DBN)

The DBN model consists of several RBM layers (Xin et al., 2018) and a Softmax classification layer. Some of the RBM is in a hidden layer on DBN which is used for training and then used again at the next training stage (Nadeem et al., 2016). DBN has two stages of training, unsupervised pretraining and supervised fine-tuning (Ranzato et al., 2009). DBN uses feature extraction and classification in detecting attacks (Alrawashdeh & Purdy, 2017) (Zhao et al., 2017).

c. Deep Neural Network (DNN)

DNN is It is an algorithm formed from many interconnected layers and is known as end-to-end machine learning. In DNN, patterns are extracted from simple feature representations with limited prior knowledge. This deep learning model is widely used in cases that cannot be solved properly by traditional machine learning algorithms (Z. Wang, 2018). A model can be trained using this neural network to perform regression and classification.

d. Recurrent Neural Network (RNN)

RNN is an artificial neural network that is designed to have sequential data. It is commonly used to perform Natural Language Processing (NLP) (Graves et al., 2013) (Graves & Jaitly, 2014). Sequential data are contextual, which means that we should not analyze sequential data separately. In order to collect contextual information, every RNN unit receives both its current status and its previous status. The direction of data flow in the RRN model is one-way flow, from one hidden unit to the next. In order for RNN to solve the problem of non-sequential data, several researchers have developed variants of RNN including long-term memory (LSTM) (Hochreiter & Urgen Schmidhuber, 1997), gated recurrent unit (GRU) (Chung et al., 2014), and bi-RNN (Schuster & Paliwal, 1997).

e. Autoencoder (AE)

Autoencoder has two components, encoder and decoder. Features are extracted from raw data using encoder. These extracted features then reconstructed by decoder. During the training process, the difference between the encoder input and the decoder output gradually decreases. Dataset does not need to be labelled because Autoencoder is unsupervised learning algorithm. If the decoder can reconstruct the data through the extracted features successfully, it can be indicated that the features extracted by the encoder describe the data substance. There are many variants of well-known autoencoders, such as denoising autoencoder (Vincent et al., 2008) (Vincent et al., 2010) and autoencoder sparse (Deng et al., 2013). Autoencoder includes neural networks that implement back-propagation (H. Lee et al., 2007).

f. Convolutional Neural Network (CNN)

The CNN algorithm is invented to imitate the human visual system, which means that CNN has an excellent performance to solve computer vision problem (Razavian et al., 2014)(Krizhevsky et al., 2012)(Lawrence et al., 1997). The CNN model consists of alternate convolution and pooling layers.

g. General Adversarial Network (GAN)

GAN is a framework for studying generative models (Goodfellow et al., 2014). There are two subnetworks of GAN model, generator and discriminator. Synthetic data which is similar to real data can be produced by generator. meanwhile and discriminator tries to differentiate between synthetic data and real data. Hence generator and discriminator support each other. GAN can learn a generative neural network that can model a training data distribution without labels. The generative network converts random input vectors into outputs similar to the training data earlier. In GAN there is a separate generative network that tries to distinguish between actual training data and sample data generated by the generative network (H. Wang & Yu, 2019).

3. Datasets

Understanding data is the foundation of deep learning methodologies. Dataset which is used in IDS must reflect the behavior of the host or network. Data sources for IDS generally come from packets, flows, sessions, and logs. It will not be easy to create a dataset and it will take a long time. However, if the dataset has been successfully created, the researcher can share the dataset. Hence, many researchers can use it without have to collect the dataset. Apart from convenience, there are other advantages of using public datasets. First of all, public datasets are reliable and recognized by other researchers which means it will produce trustworthy result. Secondly, many studies also use these datasets which allows new research result become comparable with previous research. It also possible for other authors to cite some result from the research in their paper.

Based on (Ring et al., 2019) there are 34 public datasets that can be used for Network-Based IDS which are summarized in Table 1. It can be seen from Table 1 that IDS dataset has been created since 2009, yet there are also some latest datasets which are provided by other authors. There are 3 common types of IDS dataset which are emulated traffic by software, real traffic captured from real network and synthetic traffic which is artificially generated. Some datasets were created in hours and some others were created in days or even months. When deciding which dataset should be used in research, it will be better to look at how big the dataset file size because it determines how long a deep

learning model has to trained. Thus, it will also determine how long the research must be conducted even tough author (Liu & Lang, 2019) deep learning-based model will have better performance on big dataset.

Table 1 Network Based IDS Dataset, adapted from (Ring et al., 2019)

No	Dataset	Year	Publicly Availabile	Format	Size	Duration	Traffic Type
1	AWID (Kolias et al., 2016)	2015	-	Others	37M packet	1 hour	emulated
2	Booters (Santanna et al., 2015)	2013	Yes	Packet	250GB packet	2 days	real
3	Botnet (Beigi et al., 2014)	2010/2014	Yes	Packet	14GB packet	-	emulated
4	CIC DoS (Jazi et al., 2017)	2012/2017	Yes	Packet	4.6GB packet	24 hours	emulated
5	CICIDS 2017 (Sharafaldin et al., 2017)	2017	Yes	Packet, Bi.Flow*	3.1M flows	5 days	emulated
6	CIDDS-001 (Ring et al., 2018)	2017	Yes	Uni. Flow**	32M flow	28 days	emulated & real
7	CIDDS-002 (Ring et al., 2018)	2017	Yes	Uni. Flow**	15M flow	14 days	emulated
8	CDX (Sangster et al., 2009)	2009	Yes	Packet	14 GB packet	4 days	real
9	CTU-13 (García et al., 2014)	2013	Yes	Packet, Uni. flow**, Bi. Flow*,	81M flow	125 hours	real
10	DARPA (Lippmann et al., 2000)	1998/99	Yes	Packet, log	-	7/5 weeks	emulated
11	DDoS 2016 (Alkasassbeh et al., 2016)	2016	Yes	Packet	2.1 M packet	-	synthetic
12	IRSC (Zuech et al., 2015)	2015	No	Packet, flow	-	-	real
13	ISCX 2012 (Shiravi et al., 2012)	2012	Yes	Packet, Bi. Flow*	2 M flow	7 days	emulated
14	ISOT (Saad et al., 2011)	2010	Yes	Packet	11 GB packet	-	emulated
15	KDD CUP 99 (UCI Machine Learning Repository, 2015)	1999	Yes	Others	5 M point	-	emulated
16	Kent 2016 (Kent, 2016)	2016	Yes	Uni. flow**, Logs	130 M flow	58 days	real
17	Kyoto 2006+ (Song et al., 2011)	2006-2009	Yes	Others	93 M points	3 days	real
18	LBNL (Pang et al., 2005)	2004/2005	Yes	Packet	160 M packet	5 hours	real
19	NDSec-1 (Beer et al., 2017)	2016	-	Packet, log	3.5 M packet	-	emulated
20	NGIDS-DS (Haider et al., 2017)	2016	Yes	Packet, log	1 M packet	5 days	emulated
21	NSL-KDD (Tavallaee et al., 2009)	1998	Yes	Others	150k points	-	emulated
22	PU-IDS (Singh et al., 2015)	1998	-	Others	200k points	-	synthetic
23	PUF (Sharma et al., 2018)	2018	-	Uni. flow**	300k flow	3 days	real
24	SANTA (Wheelus et al., 2014)	2014	No	Others	-	-	real
25	SSENET-2011 (Vasudevan et al., 2011)	2011	-	Others	-	4 hours	emulated
26	SSENET-2014 (Bhattacharya & Selvakumar, 2015)	2011	-	Others	200k points	4 hours	emulated
27	SSHCure (Hofstede et al., 2014)	2013/2014	Yes	Bi. flow*, Log Uni. flow**	2.4 GB flow	2 months	real
28	TRAbID (Viegas et al., 2017)	2017	Yes	Packet	460 M packet	8 hours	emulated
29	TUIDS (Bhuyan et al., 2015)	2011/2012	Yes	Packet Bi. flow*	250k flow	21 days	emulated
30	Twente (Sperotto et al., 2009)	2008	Yes	Uni. flow**	14M flows	6 days	real
31	UGR'16 (Maciá-Fernández et al., 2018)	2016	Yes	Uni. flow**	16.9G flow	4 months	real
32	UNIBS (Gringoli et al., 2009)	2009	-	Flow	79k flow	3 days	real
33	Unified Host and Network (Turcotte et al., 2017)	2017	Yes	Bi. flow* Log	150GB flow	90 days	real
34	UNSW-NB15 (Moustafa & Slay, 2015)	2015	Yes	Packet	2M point	31 hours	emulated

* Bidirectional Flow

** Unidirectional Flow

4. Frameworks

There are several frameworks which commonly used in developing deep learning models. For instance, Tensorflow, Theano, Keras, Deeplearning-4j, PyTorch, Caffe, NVIDIA cuDNN, DIGITS, MX-net and Cognitive Network Toolkit (CNTK).

TensorFlow is a distributed system and open-source framework for training Neural Networks. It was created by the Google Brain team (Abadi et al., 2016) and Google has used it since 2011.

Basically, it is a library for numerical computations. TensorFlow can run faster because it is programmed with the Python API using the C / C ++ engine. Theano is a library written in python. A Machine Learning team from Montreal University invented it to define, optimize, and perform multidimensional mathematical functions.

Keras is a framework written in Python which is developed to implement deep learning using Theano and TensorFlow. Keras provides excellent Neural Network API capabilities to implement with deep learning algorithms. Because it is based on Theano and TensorFlow, this deep learning framework is widely used and allows a platform that is extensible, modular, and easy to use by Python users (Nweke et al., 2018).

Deep learning-4j is an open-source framework for developing deep learning model. It is pre-programmed with C++, C, Scala, Java, and CUDA. Deep learning-4j is released under the Apache 2.0 license. Skymind, a startup company, has a machine learning team which developed this framework to operates on OS such as Linux, Windows, Android, and OS X (Parvat et al., 2017). The deep learning-4j framework integrates Spark and Hadoop with CPU and GPU support for fast simple modeling of DNN implementations (S. M. Lee et al., 2017).

The Torch framework can perform scientific calculations that offer various support for Machine Learning mechanisms. PyTorch is starting to be widely used in deep learning models and is considered a competitor to Tensor-Flow. PyTorch which is developed at Facebook company uses the Torch framework which is used for deep neural network construction. Caffe is developed for computer vision and machine learning. It was created by Berkeley Center with contributors in community. Its architecture is vivid with its modularity and high speed, so it can be used to design algorithms in modular way. Currently, deep learning acceleration using Caffe is supported by NVidiaGPU.

cuDNN stands for CUDA DNN, it is a library for DNN which can be accelerated using GPU. Implementation of standards such as backward convolutions, forward convolution, normalization, pooling and layer activation are carried out with good standards (highly tuned). DIGITS is a web-based tool for deep learning development which was created by NVIDIA. DIGITS uses text files to set parameters and networks. DIGITS is capable of network visualization, visualization of the learning process and has a lot of GPU support (Erickson et al., 2017).

MX-Net is a framework for deep learning and was built using C++ with multiple language bindings. It also supports distributed computing with multiple GPUs. Compared to TensorFlow and Caffe, MX-Net efficiency is on par with these framework (Erickson et al., 2017). CNTK was released in 2015 under Microsoft Research and is characterized as Visual Studio for Machine Learning. It is a much easier to use this framework for developer who has been using Visual Studio for programming. This framework usage is not as many as other previous and well-known frameworks because it is relatively new (Nweke et al., 2018).

5. Recent Researches

In Table 2, the authors have compiled several papers in this research area. In Table 2, we can make comparisons both on the dataset and the algorithm used while taking into account the year and the number of citations. From Table 2, it can be inferred that KDD99 and NSL-KDD were the most used IDS dataset for developing AI-based IDS model. On the other hand, latest dataset like CIC IDS 2017 was also used by several authors. Methods implemented in Table 2 seems vary from supervised

learning and unsupervised learning. It is recommended for authors who want to begin to do research in this area, to carefully read publication paper from each author to understand the detail of deep learning model used in the research.

Table 2. Research on Deep Learning based IDS

No	Research	Num. of Cited	Year	Author	Datasets	Methods/Algorithms
1	(Niyaz et al., 2015)	476	2016	Q. Niyaz, et al	NSL-KDD	Self-taught learning Soft-Max Regression
2	(Shone et al., 2018)	359	2018	N. Shone, et al	KDD99, NSL-KDD	DBN, S-NDAE
3	(Alrawashdeh & Purdy, 2017)	114	2016	K. Alrawashdeh & C. Purdy	KDD99	RBM, DBN2, DBN4 + LR
4	(Vinayakumar et al., 2019)	147	2019	Vinayakumar, et al	KDD99, NSL-KDD, UNSW-NB 15, WSN-DS, CI IDS 2017, Kyoto, ADFA-LD, ADFA-WD	DNN dan ML (LR, NB, KNN, DT, AB, RF, SVM-rbf
5	(Yin et al., 2017)	479	2017	C. Yin, et al	NSL-KDD	RNN
6	(Otoum et al., 2019)	77	2019	S. Otoum, et al	KDD99	RBC
7	(Z. Wang, 2018)	72	2018	Zheng Wang, et al	NSL-KDD, JSMA	DNN
8	(Al-Qatf et al., 2018)	84	2018	Majjed Al-Qatf, et al	NSL-KDD	SAE-SVM
9	(Roy et al., 2017)	64	2017	S.S. Roy, et al	KDD99	DNN
10	(Khan et al., 2019)	44	2019	F.A. Khan, et al	KDD99, UNSW-NB15	Autoencoder
11	(Papamartzivanos et al., 2019)	40	2019	Dimitrios, et al	Self-collect dataset	Autoencoder
12	(Hassan et al., 2020)	22	2020	M. Mehedi, et al	UNSW-NB15, ISCX2012	CNN, LSTM, WDLSTM
13	(Van et al., 2017)	42	2017	N.T. Van, et al	KDD99	RBM, Autoencoder
14	(Zeng et al., 2019)	33	2019	Y. Zeng, et al	ISCXVPN-nonVPN, ISCX2012	DFR, CNN, LSTM, SAE
15	(Li et al., 2017)	81	2017	Z. Li, et al	NSL-KDD	CNN
16	(Kim et al., 2016)	253	2016	J. Kim, et al	KDD99	LSTM-RNN
17	(Farahnakian & Heikkonen, 2018)	62	2018	F. Farahnakian, et al	KDD99	Deep Autoencoder
18	(Alom & Taha, 2017)	36	2017	Md.Z. Alom & T.M. Taha	KDD99	Autoencoder, RBM
19	(Yu et al., 2017)	25	2017	Y. Yu, et al	UNB ISCX IDS 2012, CTU-13	SDA-Based Deep Neural Network
20	(Ieracitano et al., 2018)	22	2018	C. Ieracitano, et al	NSL-KDD	Deep Autoencoder Shallow MLP
21	(Vinayakumar et al., 2017)	126	2017	Vinayakumar R, et al	KDD99, NSL-KDD	RNN, LSTM, CNN
22	(Yang et al., 2019)	21	2018	K. Yang, et al	KDD99, NSL-KDD	DNN, Naïve Bayes, SVM, Random Forest
23	(Ustebay et al., 2019)	22	2018	S. Ustebay, et al	CIC IDS 2017	Random Forest, MLP Classifier
24	(Zhao et al., 2017)	58	2017	G. Zhao, et al	KDD99	DBN, PNN
25	(Zhang et al., 2018)	13	2018	H. Zhanga, et al	UNSW-NB	DAE, MLP
26	(Singla et al., 2020)	2	2020	A. Singla, et al	NSL-KDD, UNSW-NB15	Adversarial Domain Adaptation
27	(Xin et al., 2018)	189	2018	Y. Xin, et al	DARPA, KDD99, NSL-KDD, ADFA	SVM, K-NN, Decision Tree, DBN, RNN, CNN
28	(Mighan & Kahani, 2020)	2	2020	S.N. Mighan & M. Kahani	UNB ISCX 2012 UNB CICIDS 2017	SAE-SVM
29	(Ding & Wang, 2018)	12	2017	S. Ding & G. Wang	KDD99	DNN
30	(Naseer et al., 2018)	98	2018	S. Naseer, et al	NSLKDDTest+ NSLKDDTest21	DNN, CNN, Autoencoder, RNN
31	(Zavrak & Iskefiyeli, 2020)	5	2020	S. Zavrak & M. Iskefiyeli	CIC IDS 2017	AE, VAE, OCSVM
32	(Gurung et al., 2019)	14	2019	S. Gurung, et al	NSL-KDD	Sparse Autoencoder with Logistic Regression

6. Research Challenges

From Table 2, we can observe that deep learning-based IDS has been researched since 2016, which means that this area is still quite new, thus providing many opportunities for other researchers who also want to conduct research in this field. This is different from Machine Learning-based IDS which has been researched for a long time and there are already a lot of research results in this field. Although the problem with deep learning is that the computation time is longer than machine learning,

the authors believe that the computing speed will be faster over time, thus in the end this will not be an obstacle anymore.

From Table 2 we can also understand that most, if not all, researchers used the DARPA, KDD Cup 99, NSL-KDD and UNSW-NB15 datasets. Even though from Table 1 we also can identify that there are lots of new datasets that have been made by other researchers. This is a challenge and also a gap for new researchers to be able to study new datasets which of course have different features from datasets which are often used. Several new datasets have more recent and varying attack patterns.

The next challenge is that researchers must also understand that many network equipment vendors have provided Intrusion Detection and Intrusion Prevention features on their devices which also have high accuracy and can automatically update the database from the vendor server (signature-based). Although this vendor may not take part in the publication of research, the existence of these tools must be realized by researchers so that the research conducted can remain relevant to the needs of science and technology.

The final challenge is how to implement the results of this study into practice by combining existing models with the IDS tools used while making regular improvements to the model.

CONCLUSIONS AND RECOMMENDATIONS

The beginning of this paper explains the urgency of developing research in the field of networks, one of which is the Intrusion Detection System (IDS). Based on the detection method, IDS consists of Anomaly-based and Signature-based (Misuse based). Based on the data source, IDS consists of Host-based IDS and Network-based IDS. Host-based IDS data sources are from logs on the host whereas network-based IDS data sources are from traffic flows, packets and sessions.

In the next section, the deep learning model often used by researchers includes: Deep Belief Network (DBN), Deep Neural Network (DNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Autoencoder, Restricted Boltzman Machine (RBM) and General Adversarial Network (GAN).

A total of 34 datasets are presented briefly in Table 1 for quick reference for those who can see what datasets are used in research in the field of Cyber Security. To help researchers, many frameworks can be used to perform deep learning computation, including: TensorFlow, Keras, Theano, Deep learning-4j, PyTorch, DIGITS, MX-net, NVIDIA cuDNN, Caffe and Cognitive Network Toolkit (CNTK). Afterwards, a table which lists research has been carried out in the field of IDS based on deep learning is presented. In the final section, paper explains what challenges researchers will undertake to conduct research in this field.

The authors hope that this paper can help to provide a brief overview of research in the field of IDS based on deep learning so that if there are researchers who are interested in conducting research, they can study research papers both in leading journals and those that become references on this paper.

REFERENCES

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., Kudlur, M., Levenberg, J., Monga, R., Moore, S., Murray, D. G., Steiner, B., Tucker, P., Vasudevan, V., Warden, P., … Zheng, X. (2016). TensorFlow: A system for large-scale machine learning. *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016*.

Aghdam, M. H., & Kabiri, P. (2016). Feature selection for intrusion detection system using ant colony optimization. *International Journal of Network Security*.

Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2869577

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*. https://doi.org/10.1016/j.knosys.2019.105124

Alkasassbeh, M., Al-Naymat, G., B.A, A., & Almseidin, M. (2016). Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. *International Journal of Advanced Computer Science and Applications*. https://doi.org/10.14569/ijacsa.2016.070159

Alom, M. Z., & Taha, T. M. (2017). Network intrusion detection for cyber security using unsupervised deep learning approaches. *Proceedings of the IEEE National Aerospace Electronics Conference, NAECON*. https://doi.org/10.1109/NAECON.2017.8268746

Alrawashdeh, K., & Purdy, C. (2017). Toward an online anomaly intrusion detection system based on deep learning. *Proceedings - 2016 15th IEEE International Conference on Machine Learning and Applications, ICMLA 2016*. https://doi.org/10.1109/ICMLA.2016.167

Anderson, J. P. (1980). Computer security threat monitoring and surveillance. *Technical Report James P Anderson Co Fort Washington Pa*. https://doi.org/citeulike-article-id:592588

Bace, R., & Mell, P. (2001). NIST special publication on intrusion detection systems. In *Nist Special Publication*.

Beer, F., Hofer, T., Karimi, D., & Bühler, U. (2017). A new attack composition for network security. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*.

Beigi, E. B., Jazi, H. H., Stakhanova, N., & Ghorbani, A. A. (2014). Towards effective feature selection in machine learning-based botnet detection approaches. *2014 IEEE Conference on Communications and Network Security, CNS 2014*. https://doi.org/10.1109/CNS.2014.6997492

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. In *Information (Switzerland)* (Vol. 10, Issue 4). https://doi.org/10.3390/info10040122

Bhattacharya, S., & Selvakumar, S. (2015). SSENet-2014 Dataset: A Dataset for Detection of Multiconnection Attacks. *Proceedings - 2014 3rd International Conference on Eco-Friendly Computing and Communication Systems, ICECCS 2014*. https://doi.org/10.1109/Eco-friendly.2014.100

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). Towards generating real-life datasets for network intrusion detection. *International Journal of Network Security*.

Chung, J., Gülçehre, Ç., Cho, K., & Bengio, Y. (2014). Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling. *CoRR*, *abs/1412.3*. http://arxiv.org/abs/1412.3555

CyberEdge Group. (2020). *2020 Cyberthreat Defense Report*. https://cyber-edge.com/cdr/

Deng, J., Zhang, Z., Marchi, E., & Schuller, B. (2013). Sparse autoencoder-based feature transfer learning for speech emotion recognition. *Proceedings - 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction, ACII 2013*. https://doi.org/10.1109/ACII.2013.90

Ding, S., & Wang, G. (2018). Research on intrusion detection technology based on deep learning. *2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017*. https://doi.org/10.1109/CompComm.2017.8322786

Drewek-Ossowicka, A., Pietrołaj, M., & Rumiński, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1).

https://doi.org/10.1007/s12652-020-02014-x

Erickson, B. J., Korfiatis, P., Akkus, Z., Kline, T., & Philbrick, K. (2017). Toolkits and Libraries for Deep Learning. In *Journal of Digital Imaging*. https://doi.org/10.1007/s10278-017-9965-6

Farahnakian, F., & Heikkonen, J. (2018). A deep auto-encoder based approach for intrusion detection system. *International Conference on Advanced Communication Technology, ICACT*. https://doi.org/10.23919/ICACT.2018.8323688

Fulkerson, B., Michie, D., Spiegelhalter, D. J., & Taylor, C. C. (1995). *Machine Learning, Neural and Statistical Classification*. Technometrics. https://doi.org/10.2307/1269742

Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, *169*. https://doi.org/10.1016/j.jnca.2020.102767

García, S., Grill, M., Stiborek, J., & Zunino, A. (2014). An empirical comparison of botnet detection methods. *Computers and Security*. https://doi.org/10.1016/j.cose.2014.05.011

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*. https://doi.org/10.3156/jsoft.29.5_177_2

Graves, A., & Jaitly, N. (2014). Towards end-to-end speech recognition with recurrent neural networks. *31st International Conference on Machine Learning, ICML 2014*.

Graves, A., Mohamed, A. R., & Hinton, G. (2013). Speech recognition with deep recurrent neural networks. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*. https://doi.org/10.1109/ICASSP.2013.6638947

Gringoli, F., Salgarelli, L., Dusi, M., Cascarano, N., Risso, F., & Claffy, K. C. (2009). GT: Picking up the truth from the ground for internet traffic. *Computer Communication Review*. https://doi.org/10.1145/1629607.1629610

Gurung, S., Kanti Ghose, M., & Subedi, A. (2019). Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset. *International Journal of Computer Network and Information Security*. https://doi.org/10.5815/ijcnis.2019.03.02

Haider, W., Hu, J., Slay, J., Turnbull, B. P., & Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2017.03.018

Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M., & Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences*. https://doi.org/10.1016/j.ins.2019.10.069

Heberlein, L. T., Dias, G. V, Levitt, K. N., Mukherjee, B., Wood, J., & Wolber, D. (1989). *A network security monitor*. https://doi.org/https://doi.org/10.2172/6223037

Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.3000179

Hochreiter, S., & Urgen Schmidhuber, J. J. (1997). Long short term memory. Neural computation. *MEMORY Neural Computation*.

Hofstede, R., Hendriks, L., Sperotto, A., & Pras, A. (2014). SSH compromise detection using NetFlow/IPFIX. *Computer Communication Review*. https://doi.org/10.1145/2677046.2677050

Ieracitano, C., Adeel, A., Gogate, M., Dashtipour, K., Morabito, F. C., Larijani, H., Raza, A., & Hussain, A. (2018). Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and*

Lecture Notes in Bioinformatics). https://doi.org/10.1007/978-3-030-00563-4_74

Jazi, H. H., Gonzalez, H., Stakhanova, N., & Ghorbani, A. A. (2017). Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Computer Networks*. https://doi.org/10.1016/j.comnet.2017.03.018

Kent, A. D. (2016). Cyber security data sources for dynamic network research. In *Dynamic Networks and Cyber-Security*. https://doi.org/10.1142/9781786340757_0002

Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). TSDL: A Two-Stage Deep Learning Model for Efficient Network Intrusion Detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2899721

Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016). Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection. *2016 International Conference on Platform Technology and Service, PlatCon 2016 - Proceedings*. https://doi.org/10.1109/PlatCon.2016.7456805

Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys and Tutorials*. https://doi.org/10.1109/COMST.2015.2402161

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*. https://doi.org/10.1061/(ASCE)GT.1943-5606.0001284

Lawrence, S., Giles, C. L., Tsoi, A. C., & Back, A. D. (1997). Face recognition: A convolutional neural-network approach. *IEEE Transactions on Neural Networks*. https://doi.org/10.1109/72.554195

Lee, H., Battle, A., Raina, R., & Ng, A. Y. (2007). Efficient sparse coding algorithms. *Advances in Neural Information Processing Systems*. https://doi.org/10.7551/mitpress/7503.003.0105

Lee, S. M., Yoon, S. M., & Cho, H. (2017). Human activity recognition from accelerometer data using Convolutional Neural Network. *2017 IEEE International Conference on Big Data and Smart Computing, BigComp 2017*. https://doi.org/10.1109/BIGCOMP.2017.7881728

Li, Z., Qin, Z., Huang, K., Yang, X., & Ye, S. (2017). Intrusion detection using convolutional neural networks for representation learning. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-70139-4_87

Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., Weber, D., Webster, S. E., Wyschogrod, D., Cunningham, R. K., & Zissman, M. A. (2000). Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. *Proceedings - DARPA Information Survivability Conference and Exposition, DISCEX 2000*. https://doi.org/10.1109/DISCEX.2000.821506

Maciá-Fernández, G., Camacho, J., Magán-Carrión, R., García-Teodoro, P., & Therón, R. (2018). UGR'16: A new dataset for the evaluation of cyclostationarity-based network IDSs. *Computers and Security*. https://doi.org/10.1016/j.cose.2017.11.004

Mighan, S. N., & Kahani, M. (2020). A novel scalable intrusion detection system based on deep learning. *International Journal of Information Security*. https://doi.org/10.1007/s10207-020-00508-5

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*. https://doi.org/10.1109/MilCIS.2015.7348942

Nadeem, M., Marshall, O., Singh, S., Fang, X., & Yuan, X. (2016). Semi-Supervised Deep Neural Network for Network Intrusion Detection. *Research and Practice*.

Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2863036

Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015). A deep learning approach for network intrusion detection system. *EAI International Conference on Bio-Inspired Information and Communications Technologies (BICT)*. https://doi.org/10.4108/eai.3-12-2015.2262516

Nweke, H. F., Teh, Y. W., Al-garadi, M. A., & Alo, U. R. (2018). Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges. In *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2018.03.056

Otoum, S., Kantarci, B., & Mouftah, H. T. (2019). On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Networking Letters*. https://doi.org/10.1109/lnet.2019.2901792

Pang, R., Allman, M., Bennett, M., Lee, J., Paxson, V., & Tierney, B. (2005). A first look at modern enterprise traffic. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*. https://doi.org/10.1145/1330107.1330110

Papamartzivanos, D., Gomez Marmol, F., & Kambourakis, G. (2019). Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2893871

Parvat, A., Chavan, J., Kadam, S., Dev, S., & Pathak, V. (2017). A survey of deep-learning frameworks. *Proceedings of the International Conference on Inventive Systems and Control, ICISC 2017*. https://doi.org/10.1109/ICISC.2017.8068684

Ranzato, M., Boureau, Y. L., & Le Cun, Y. (2009). Sparse feature learning for deep belief networks. *Advances in Neural Information Processing Systems 20 - Proceedings of the 2007 Conference*.

Razavian, A. S., Azizpour, H., Sullivan, J., & Carlsson, S. (2014). CNN features off-the-shelf: An astounding baseline for recognition. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*. https://doi.org/10.1109/CVPRW.2014.131

Ring, M., Landes, D., & Hotho, A. (2018). Detection of slow port scans in flow-based network traffic. *PLoS ONE*. https://doi.org/10.1371/journal.pone.0204507

Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. In *Computers and Security*. https://doi.org/10.1016/j.cose.2019.06.005

Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2017). A deep learning based artificial neural network approach for intrusion detection. *Communications in Computer and Information Science*. https://doi.org/10.1007/978-981-10-4642-1_5

Saad, S., Traore, I., Ghorbani, A., Sayed, B., Zhao, D., Lu, W., Felix, J., & Hakimian, P. (2011). Detecting P2P botnets through network behavior analysis and machine learning. *2011 9th Annual International Conference on Privacy, Security and Trust, PST 2011*. https://doi.org/10.1109/PST.2011.5971980

Sangster, B., O'Connor, T. J., Cook, T., Fanelli, R., Dean, E., Adams, W. J., Morrell, C., & Conti, G. (2009). Toward instrumenting network warfare competitions to generate labeled datasets. *2nd Workshop on Cyber Security Experimentation and Test, CSET 2009*.

Santanna, J. J., Van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters - An analysis of DDoS-as-a-service attacks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*. https://doi.org/10.1109/INM.2015.7140298

Schuster, M., & Paliwal, K. K. (1997). Bidirectional recurrent neural networks. *IEEE Transactions on Signal Processing*. https://doi.org/10.1109/78.650093

Sharafaldin, I., Gharib, A., Lashkari, A. H., & Ghorbani, A. A. (2017). Towards a Reliable Intrusion Detection Benchmark Dataset. *Software Networking*. https://doi.org/10.13052/jsn2445-

9739.2017.009

Sharma, R., Singla, R. K., & Guleria, A. (2018). A New Labeled Flow-based DNS Dataset for Anomaly Detection: PUF Dataset. *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2018.05.079

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers and Security*. https://doi.org/10.1016/j.cose.2011.12.012

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*. https://doi.org/10.1109/TETCI.2017.2772792

Singh, R., Kumar, H., & Singla, R. K. (2015). A reference dataset for network traffic activity based intrusion detection system. *International Journal of Computers, Communications and Control*. https://doi.org/10.15837/ijccc.2015.3.1924

Singla, A., Bertino, E., & Verma, D. (2020). Preparing Network Intrusion Detection Deep Learning Models with Minimal Data Using Adversarial Domain Adaptation. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2020*. https://doi.org/10.1145/3320269.3384718

Song, J., Takakura, H., Okabe, Y., Eto, M., Inoue, D., & Nakao, K. (2011). Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation. *Proceedings of the 1st Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2011*. https://doi.org/10.1145/1978672.1978676

Sperotto, A., Sadre, R., Van Vliet, F., & Pras, A. (2009). A labeled data set for flow-based intrusion detection. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-04968-2_4

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*. https://doi.org/10.1109/CISDA.2009.5356528

Turcotte, M. J. M., Kent, A. D., & Hash, C. (2017). Unified host and network data set. In *arXiv*. https://doi.org/10.1142/9781786345646_001

UCI Machine Learning Repository. (2015). KDD Cup 1999 Data. In *1999]. Http://Kdd. Ics. Uci. Edu/Databases/Kddcup99/Kddcup99. Html*.

Ustebay, S., Turgut, Z., & Aydin, M. A. (2019). Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier. *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings*. https://doi.org/10.1109/IBIGDELFT.2018.8625318

Van, N. T., Thinh, T. N., & Sach, L. T. (2017). An anomaly-based network intrusion detection system using Deep learning. *Proceedings - 2017 International Conference on System Science and Engineering, ICSSE 2017*. https://doi.org/10.1109/ICSSE.2017.8030867

Vasudevan, A. R., Harshini, E., & Selvakumar, S. (2011). SSENet-2011: A Network Intrusion Detection System dataset and its comparison with KDD CUP 99 dataset. *Asian Himalayas International Conference on Internet*. https://doi.org/10.1109/AHICI.2011.6113948

Viegas, E. K., Santin, A. O., & Oliveira, L. S. (2017). Toward a reliable anomaly-based intrusion detection in real-world environments. *Computer Networks*. https://doi.org/10.1016/j.comnet.2017.08.013

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2895334

Vinayakumar, R., Soman, K. P., & Poornachandrany, P. (2017). Applying convolutional neural network

for network intrusion detection. *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*. https://doi.org/10.1109/ICACCI.2017.8126009

Vincent, P., Larochelle, H., Bengio, Y., & Manzagol, P. A. (2008). Extracting and composing robust features with denoising autoencoders. *Proceedings of the 25th International Conference on Machine Learning*. https://doi.org/10.1145/1390156.1390294

Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y., & Manzagol, P. A. (2010). Stacked denoising autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion. *Journal of Machine Learning Research*.

Wang, H., & Yu, C. N. (2019). A Direct Approach to Robust Deep Learning Using Adversarial Networks. In *arXiv*.

Wang, Z. (2018). Deep Learning-Based Intrusion Detection with Adversaries. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2854599

Wheelus, C., Khoshgoftaar, T. M., Zuech, R., & Najafabadi, M. M. (2014). A session based approach for aggregating network traffic data - The SANTA dataset. *Proceedings - IEEE 14th International Conference on Bioinformatics and Bioengineering, BIBE 2014*. https://doi.org/10.1109/BIBE.2014.72

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2836950

Yang, K., Liu, J., Zhang, C., & Fang, Y. (2019). Adversarial Examples Against the Deep Learning Based Network Intrusion Detection Systems. *Proceedings - IEEE Military Communications Conference MILCOM*. https://doi.org/10.1109/MILCOM.2018.8599759

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2017.2762418

Yu, Y., Long, J., & Cai, Z. (2017). Session-based network intrusion detection using a deep learning architecture. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-67422-3_13

Zavrak, S., & Iskefiyeli, M. (2020). Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.3001350

Zeng, Y., Gu, H., Wei, W., & Guo, Y. (2019). Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2908225

Zhang, H., Wu, C. Q., Gao, S., Wang, Z., Xu, Y., & Liu, Y. (2018). An Effective Deep Learning Based Scheme for Network Intrusion Detection. *Proceedings - International Conference on Pattern Recognition*. https://doi.org/10.1109/ICPR.2018.8546162

Zhao, G., Zhang, C., & Zheng, L. (2017). Intrusion detection using deep belief network and probabilistic neural network. *Proceedings - 2017 IEEE International Conference on Computational Science and Engineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, CSE and EUC 2017*. https://doi.org/10.1109/CSE-EUC.2017.119

Zuech, R., Khoshgoftaar, T. M., Seliya, N., Najafabadi, M. M., & Kemp, C. (2015). A new intrusion detection benchmarking system. *Proceedings of the 28th International Florida Artificial Intelligence Research Society Conference, FLAIRS 2015*.