The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

A Review of Intrusion Detection Systems: Techniques, Methodologies and Approaches

D.Chaithanya KumarA[1]. Sumathi[2], B Satish Kumar[3], P. Lalitha[4], B. Bhavya Harshita[5]
[1]Department of Computer Science, S.G.S Arts Collage(A) T.T.D, Tirupathi, AP, India
[2]Department of Computer Science, GDCW Degree College SKHT, Srikalahasti, AP, India
[3]Department of Computer Science, SVA Degree College SKHT, Srikalahasti, AP, India
[4,5]Department of CSE, Lendi Institute of Engineering and Technology,
Vizianagaram, India.

Abstract

Cybercrime and cyberattacks are becoming increasingly common these days. Networks must be protected from these increasingly complex threats by both individuals and organizations. These intrusions and attacks target the security services provided by network security, including confidentiality, integrity, and availability. An Intrusion Detection and Prevention System (IDPS) is a piece of software designed to identify assaults against an application or network infrastructure. The significance of IDPS has significantly increased due to the rise in cybercrime and the increased exposure to harmful content in the digital realm. This review's objective is to identify and assess the different techniques, strategies, and tactics used in intrusion detection systems. Numerous intrusion detection methods are proposed in the literature. These systems control a range of network attacks and threats. They can be divided into three groups: anomaly-based IDS, signature-based IDS, and network behavioral IDS. In this review, we look at and assess a number of methods that have been published in the literature to ascertain their goals and possible directions for future study.

Keywords:
Anomaly based IDS, Attacks, Intrusion Detection System, Signature based IDS.

1. Introduction

In recent years, the size of computer networks has increased dramatically. Information, communication, and hosts are the parts of the computer network that are always expanding. The exponential growth of security system vulnerabilities poses significant threats. Threats that disrupt the system's normal operation are dangerous and lead to the loss of crucial information and company resources. Firewalls, anti-virus software, behavioral analytics, spam filters, access control, denial of service (DoS), distributed denial of service (DDoS), anti-malware software, application security, data loss, and network segmentation are just a few of the techniques that organizations regularly use to enhance network security. They are useless and usually unable to protect the network against internal threats and unexpected attacks because they are usually used with simple rules-based algorithms and generate a table that allows or prohibits IP addresses

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

or access to particular ports. Because of this, they are unable to distinguish between legal and fraudulent communications and are unable to stop sophisticated assaults like DoS (Denial of Service).

The act of monitoring system events and analyzing them to search for intrusions is known as intrusion detection, according to the National Institute of Standards and Technology (NIST). However, techniques for detecting and thwarting network attacks need to be updated frequently due to the dynamic nature of today's cyber environment. Snort and Suricata are the two most popular and commonly used IDSs. Unlike Snort, which was created by Martin Roesch in 1998 and later acquired by Cisco, Suricata was created by the Open Information Security Foundation in 2010. An intrusion detection system is a piece of software that helps with host and network security by automating the process of intrusion detection through network traffic monitoring. IDSs can detect possible network attacks, both known and unknown. An intrusion detection system (IDS) can be classified into multiple types.

1. Intrusion Detection System (HIDS) based on the host
2. Systems for detecting network intrusions (NIDS)
3. WIDS (Wireless Intrusion Detection System)
4. Analysis of Network Behavior (NBA)

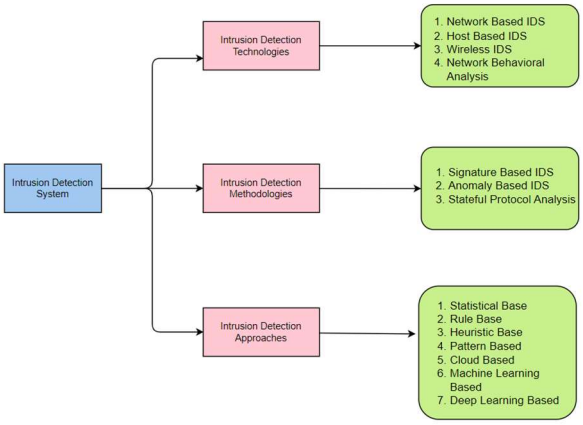

Fig. 1. Intrusion Detection Systems – Technologies, Methodologies and Approaches

Host Based Intrusion Detection Systems (HIDS) detect anomalous traffic at the host level. They can detect and thwart system-level threats when used with NIDS. Network Intrusion Detection Systems (NIDS) specialize in security against these threats. All network traffic is examined, any suspicious behavior is reported, and the system is prevented from being harmed. Wireless Intrusion Detection Systems (WIDS) monitor network traffic in wireless networks by looking at the traffic in wireless network protocols in order

to identify intrusion risks. Despite its inability to identify suspicious data in upper layer protocols like TCP and UDP, it is widely utilized in wireless network coverage areas.
Network Behavioral Analysis (NBA) tools look at network statistics to find anomalous network traffic flows. These anomalies indicate the presence of malware or attacks such as Distributed Denial of Service (DDoS). NBA systems also employ sensors, controllers, and administrative servers. They provide event management tools in addition to network security. An intrusion detection system acts as a vigilant guardian. Its purpose is to detect any illegal conduct and to raise an alarm when any suspicious activity is discovered. Security personnel hear this clear and urgent alert, or it triggers automatic response systems, which leads to prompt action. The system maintains comprehensive activity logs that help with intrusion profile generation and post-incident analysis.

Managing the log formats and comparing them with identified patterns is one of the primary issues in IDS. The primary objective of this literature is to identify research trends in intrusion detection utilizing various methodologies and methodology. A comparison of several databases and search engines was part of this paper. Web Science, Microsoft Academic, Google Scholar, and other search engines are a few examples. Microsoft Academic has published 261,445,825 authors, 743,427 themes, 4,523 conferences, 48,974 journals, and 25,811 institutions.

The remaining portion of the study is devoted to Section IV, which addresses the Network Intrusion Detection System, Section III, which discusses methodologies, and Section II, which covers related NIDS work. Section V covers the datasets used in NIDS; Section VI covers the methodologies employed in NIDS; Section VII covers performance measurement; and Section VIII presents the conclusion.

2. Literature Survey

Many surveys on intrusion detection have been carried out over the last ten years. Bishop gave one of the earliest talks on current trends in intrusion detection and vulnerability research [1]. The most recent intrusion detection standards and infrastructure-based methodologies are needed to create and implement intrusion detection algorithms.

In order to develop a signature-based attack detection system, Sangwan and Kumar [2] proposed using Snort IDS with Debian. This intrusion detection system will capture real-time network traffic and analyze network intrusions. False positives are rare as long as the assaults are clearly stated beforehand. It is more challenging to identify unknown attacks early on. They concluded that their system could detect and assess intrusions in real-time network traffic. In order to pave the way for an intrusion detection and prevention system, they proposed developing a prototype that would automatically filter, eliminate, and quarantine the intrusion in real-time network traffic.

An important survey of machine learning techniques for intrusion detection was presented by Zamani and Movahedi [3]. Zamani evaluated the benefits of employing a machine learning approach for intrusion detection, which include rapid adaptability to changing intrusive behavior, a low false-positive rate, and a high detection rate. The algorithms examined in this review study are found in databases related to artificial intelligence (AI) and computational intelligence (CI).

Yang and McLaughlin et al. [4] proposed stateful intrusion detection for IEC 60870-5-104 SCADA security. They created a stateful intrusion detection system (IDS) that employed the Deep Packet Inspection technique to improve the security of SCADA systems. This technique was developed specifically for the IEC 60870-5-104 protocol. DFM is used to characterize both usual and important protocol behavior as well as protocol misbehavior in the form of alarm states.

Several data mining methods for intrusion detection were investigated by Agrawal and Agrawal [5]. Information retrieval systems (IDSs) have made extensive use of a range of machine learning approaches, either alone or in combination, for feature selection and dimensionality reduction in addition to clustering and classification.

New techniques based on bioinspired approaches are included into the statistical method in contemporary IDS approaches. These techniques are primarily inspired by evolutionary theory and the swarm intelligence methodology [6]. A variety of parameters, such as convergence, intensification, diversification, CPU time, etc., must be considered in order to determine the most appropriate and best-fit selection of bio-inspired algorithms.

Ahmed et al. [7] looked at the IDS categories of classification, statistics, information theory, and clustering as well as the problems with the datasets utilized for the IDS Model.

Gendreau and Moorman [8] examined intrusion detection systems (IDS) in order to develop an end-to-end secure Internet of things (IoT). This IDS survey proposes the current IoT using the newest concepts and techniques. The current research trend towards a universal, cross-platform dispersed strategy has been taken into consideration in order to comprehend and show the distinctions amongst IDS platforms.

Hamid et al. provided a summary of the benchmark datasets that intrusion detection researchers may use to train and evaluate their models [9]. Among the datasets that were examined were ADFA-WD (Australian Defense Force Academy Window Dataset), Caida DDoS (Caida Distributed denial of service) Dataset, UNM-Dataset, UNSW-NW15, DARPA 98, KDD'99, NSL-KDD, and UNM-Dataset.

The most recent proposal for a thorough examination and analysis of machine learning techniques for intrusion detection was provided by Mishra et al. [10]. This survey uses four types of classifiers: multiple classifiers with all the characteristics of the dataset, multiple classifiers with some of the features of the

dataset, single classifiers with all the features of the dataset, and single classifiers with only part of the features of the dataset. Additionally, this study shows that an intrusion detection technique that works well against one kind of attack can not work as well against another.
Qassim and Zin et al. proposed an anomaly classification technique for a network-based intrusion detection system [11]. They concluded that Random Committee and Random Tree were effective in classifying the identified activities after examining a number of machine learning algorithms on various datasets, including Random Committee, Rotation Forest, PART, Random Forest, and Random Tree. They also proposed an AIDS alarm classifier based on machine learning. This classifier automatically classifies activities discovered by an anomaly detection system based on packet headers. The proposed future work includes classifying the detected activity using a random committee technique for more precision.

The study trend and popularity in the NIDS based on specific statistical markers are not addressed in any of the literature that has been studied thus far. But in this article, we'll examine a range of commercially available intrusion detection systems, the broad adoption of several benchmark datasets, and new developments in intrusion detection techniques. Instead than using qualitative measurements, the analysis in this article is based on quantitative ones.

3. Methodology

Articles with a lot of references attract researchers. In order to assess the caliber and dependability of a research topic or journal articles in a field of study, we used references as a metric. In the third section, string-based searching was used to find academic articles published between 2010 and 2021.

The "Microsoft Academic" advanced search uses keywords associated with anomaly detection, bio-inspired algorithms, and intrusion detection systems, according to the network intrusion detection model. Terms pertaining to datasets, techniques, issues, and intrusion detection systems are also used. Table 1 lists the search term for datasets, methods, and their subclasses.

Studies for various methods used in intrusion detection systems are analyzed using filters investigated between 2010 and 2021. The search parameters "oldest first" and "intrusion detection system" have been applied. The search terms for performance metrics are further restricted by popular topics like "False positive rate," "True positive rate," and "F1 score". The same filters are used in both the analysis of the entire paper and the reference evaluation of various intrusion detection methods. Articles published between 2010 and 2021 provided the study's data. To minimize daily reference variations, we are retaining published article data beyond 2021.

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

Table 1. The searching string on which research articles from the year 2010 to 2021 are chosen.

Searching base	Searched strings
Datasets	"KDD Cup'99" + "intrusion detection", "NSL-KDD" +"intrusion detection", "Kyoto 2006" + "intrusion detection", "UNSW-NB15" + "intrusion detection", "SSENet" + "intrusion detection", "ISCX" + "intrusion detection", and "CIDDS" + "intrusion detection".
Approaches used in IDS	"Statistical based" + "Intrusion detection", "Knowledge based" + "Intrusion detection", "Machine Learning Based" + "intrusion detection", and "Bio-inspired based" + "Intrusion detection" **Statistical-based NIDS approaches** "Univariate" + "intrusion detection", "Multivariate" + "intrusion detection", "Time series" + "intrusion detection". **Knowledge-based NIDS approaches** "Finite state machine" + "intrusion detection" || "FSM" + "intrusion detection", "Description Language" + "Intrusion detection", "Expert System" + "Intrusion detection". **Machine learning-based NIDS approaches** "Linear regression" + "intrusion detection", "Logistic regression" + "intrusion detection", "Decision tree" + "intrusion detection", "K-mean" + "intrusion detection", "Neural network" + "intrusion detection", "KNN" + "intrusion detection", "SVM" + "intrusion detection" || "support vector machine" + "intrusion "Principal component analysis" + "intrusion detection" || "PCA" + "intrusion detection", "AdaBOOST" + "intrusion detection", "Gradient BOOST" + "intrusion detection", "clustering" + "intrusion detection" || "outlier" + "intrusion detection".
Performance measure-ments	"Confusion matrix", "Receiver operating characteristic". "Confusion matrix" && "intrusion detection system", "Receiver operating characteristic" && "intrusion detection system", "misclassification rate" && "intrusion detection system". "Accuracy" && "intrusion detection system", "True positive rate" && "intrusion detection system" || "recall" && "intrusion detection system" || "sensitivity" && "intrusion detection system", "true negative rate" && "intrusion detection system" || "Specificity" && "intrusion detection system", "Precision" && "intrusion

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

	detection system", "false positive rate" && "intrusion detection system", "Prevalence" && "intrusion detection system", "F-Score" && "intrusion detection system"

4. Network Intusion System

James P. Anderson voiced concerns about growing security issues in a 1972 report [12]. In 1980, he developed an audit-based method for host monitoring and automated intrusion detection. Between 1980 and 1990, the US government funded several projects, such as Discovery, Multics intrusion detection and alerting system (MIDAS), Network Audit Director and Intrusion Reporter (NADIR), and Haystack.

Zuech et al. [13] investigated how an NIDS enhances forensics' capacity to identify breach tracks. Attacks spread from one machine in a network to another via switches and routers. A network intrusion detection system (NIDS) keeps an eye on network traffic data at routers or switches at OSI layer 3 (network layer). The NIDS can be further classified as Anomaly (Unknown)-Based or Misuse (Known)-Based IDS based on pattern matching of network traffic data. Using a pattern-based examination of traffic flow, anomaly detection infers intrusive information when expected pattern behavior deviates.

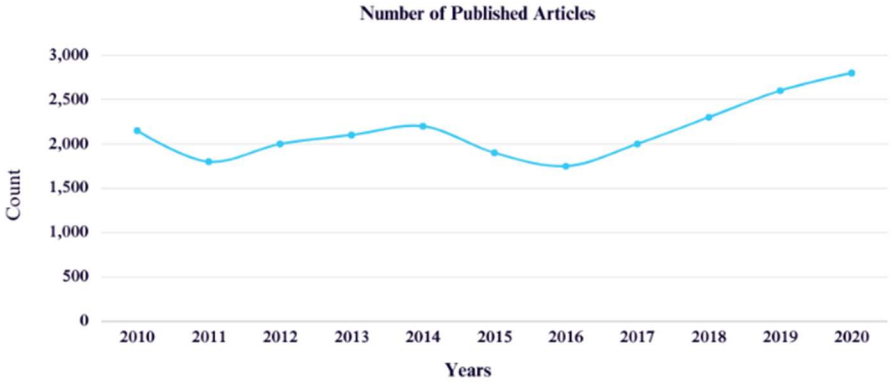

Fig 2. Publication on Intrusion Detection System from 2010 to 2020

The image above graphically depicts a year-by-year examination of intrusion detection articles published between 2010 and 2020. Over the past ten years, there has been a steady increase in publications related to research and intrusion detection.

The various NIDS modules are depicted in Figure 2. These modules carry out a network's invasive information detection function. The three NIDS modules' respective functions are displayed collectively. The identifying machines module can be used to identify anomalies or intrusions. The management machine

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

oversees the detection strategies or policies while the detection program executes the detection approaches. The data capture module is one of the detecting machine module's other sub-modules.

Network packets are recorded by the intrusion detection and communication modules. The second module of a conventional NIDS, the Management Machine, is in charge of overseeing and upholding detection policies based on detection techniques. The third module, the database, logs and tracks intrusion detection activities based on features.

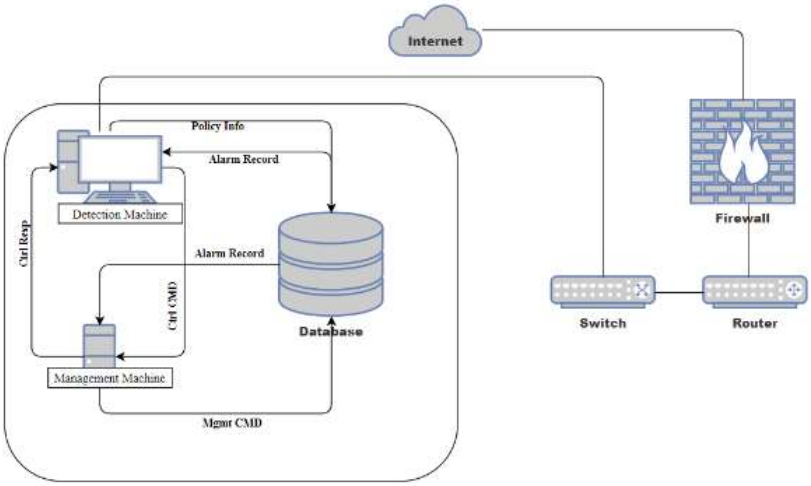

Figure 1.1 Components of NIDS

A. Causes Of Intrusion in Network

We identified a few typical reasons for network infiltration based on Anchugam and Thangadurai [14] and Ghorbani et al. [15]. A list of these is provided below.

1. Missing local packets and faulty packets (produced by defective DNS data or software defects) may result in a substantial false-alarm rate (false positive).

2. Encrypted packets may result in unavoidable invasions in the absence of an efficient intrusion detection system.

3. IDS may not be able to suggest identification and authentication for network poor access. When an attacker gains access through a soft authentication mechanism, IDS acts as a deterrent.

4. NIDS systems may fail due to Transmission Control Protocol/Internet Protocol (TCP/IP) stack assaults, and hosts within the network may become vulnerable to illicit data due to protocol-based attacks against NIDS systems.

B. Comparisons of some popular NIDS

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

There are numerous NIDS that are commercially utilized for network security. Table 2 lists some popular NIDSs and their comparative analysis.

Table 2: Commonly used Intrusion Detection Systems

S. No	NIDS	Manufacturer	Approaches used	Advantage
1	Snort created by martin Roesch, 1998 [16]	Cisco systems, sourcefire https://www.snort.org/	Signature-based, network intrusion detection, pattern matching algorithm.	Free open-source, real-time alerting, and packet logging
2	OSSec: Open-source HIDS security Daniel b. Cid owned the copyrights of the OSSec project, 2008.	Alienvault® ossim in 2008 currently maintained by atomicorp https://atomicorp.com/ about-ossec/	Correlate and analyze logs, log-based intrusion detection	File integrity monitoring (FIM), log monitoring, rootkit detection, auditing, export to SIEMs, active response, pro- cess monitoring, time-based alerting, and log analysis
3	Ossim open-source security information and event management (SIEM)	Alien vault ossim™ in 2008 currently, at &t cybersecurity in 2019	Log processing, correlation directives (rules), behavioral monitoring, SIEM event correlation	Lacks support for cloud-based servers and applications reports are heavy and detailed. And tedious to parse through
4	Suricata free and open-source, a real-time intrusion detection system	Owned and supported by the open information security foundation (OISF) www.openinfosecfoundation. Org	Signature-based intrusion detection, process multithreading to improve pro- cessing speed [17]	Suricata can handle larger volumes of traffic as compared to snort
5	Bro: an open-source software frame-work that detect behavioral	Initially written by vern pax-son later in 2018, paxson and the project's leadership team gave a new name to this	Script interpretation	Transforms network traffic data into higher-level events. Offers a script interpreter

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

	abnomalities on a network	project zeek for developing the ids. Like suricata or snort, it is also rules-based ids. Https://bricata.com/blog/ what-is-bro-ids/		
6	Fragroute/fragrouter: a network intrusion detection eva- sion toolkit	D. Son https://monkey.org/ ~dugsong/fragroute/	When Fragroute initialize, it deletes the route to the target intercepts network traffic and modifies the packets before forwarding	Probe packets can be fragmented easily with fragrout icmp echo request messages are used by fratest
7	Base: basic analysis and security engine (base) offers a web-based front end for examining the alerts produced by snort.	Https://sourceforge.net/ projects/secureideas/	It offers a web front-end to query and analysis the alerts produced by a snort IDS.	User authentication and role-based system search interface and query-builder for identical alerts matching from the alert meta information packet viewer (decoder)
8	Sguil: built by a group named network security analysts	Https://github.com/bammv/ sguil/releases/tag/v0.9.0	Event-driven analysis network security monitoring	Captures raw packet, session data, and real-time events compatible on the operating system that supports tcl/tk receive alerts from ossec, Zeek, Suricata, snort, and other data sources.

5. Benchmark datasets used in NIDS models

Several benchmark datasets were used to evaluate the intrusion detection model. Project Fig. 3 displays the annual distribution of citations for several datasets between 2010 and 2020.The goal of the work on the various datasets is to improve classification accuracy and detection rate [18]. Numerous intrusion detection

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

datasets have been made available in recent years. Finding an appropriate dataset to test an intrusion detection algorithm is difficult. Ring et al. [19] evaluated and examined the properties, assault scenarios, and interrelationships of the existing datasets for network-based intrusion detection.

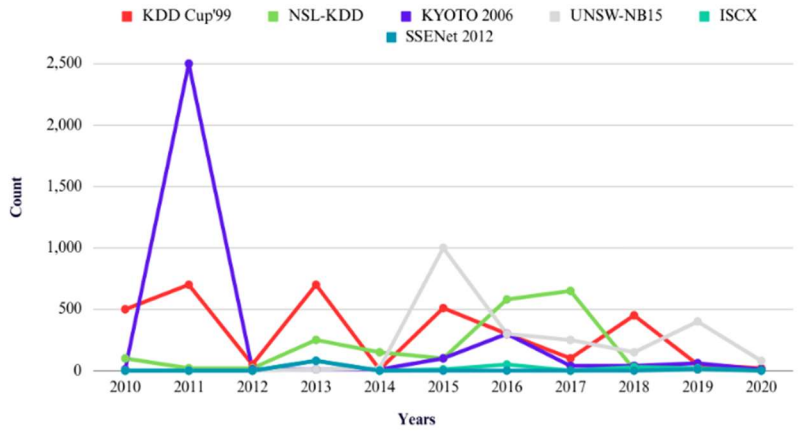

Fig 3. Year-wise distribution of the citation for different datasets from the year 2010 to 2020.

Table 3: Datasets used in NIDS

S. No.	Datasets	Advantages	Disadvantages
1	KDD CUP'99 KDD stands for Knowledge Discovery in Databases https://bit.ly/3wSG5YA	Extensive repository of attack vectors, Large amount of attacks	Obsolete in fixing of many attacks It does not provide real attack data
2	NSL- KDD: NSL-KDD is an updated version of the KDD cup99 data set where NSL stands for Network Security Laboratory http://205.174.165.80/CICDataset/ NSL-KDD/	No duplicate data found within the NSL-KDD train dataset and Test set Contains a reasonable number of samples by train and test sets	According to McHugh et al. [20] NSL-KDD may not represent real network flow
3	UNSW-NB15 Dataset: https://bit.ly/2Q1k895	Separate training and test set 45 Distinct IP addresses Publicly available	UNSW-NB15 datasets contain a limited number of attacks and no attacks related to cloud computing, like SQL injection Imbalanced training and testing classes

4	Kyoto 2006+ : https://bit.ly/3gL.f7vo	14 attributes are the same as in KDD CUP 99. besides 10 new attributes Provides real attack data	Limited volume of 'normal' traffic and 'Nor- mal' data is unrealistic that makes it a low backdrop for the attack data Normal traffic records
5	ISCX 2012 Dataset: ISCX stands for Information Security Center of Excellence https://bit.ly/2R19o5B	Up-to-date dataset compared to the other commonly datasets Representative of real network traffic Dynamic, scalable, reproducible, and labeled benchmark dataset	ISCX-2012 does not comprise any novel traffic attributes or session-based records Due to its unidirectional nature, it is challenging to the buried context in the payload data
6	SSENet 2012 Dataset: (Unknown link)	Generated in a real network environment	Unknown
7	CIDDS-001 Dataset: The University of Coburg published CIDDS (Coburg Intrusion Detection Data Sets) https://bit.ly/3mLQAYT	Contains detailed metadata for more in-depth investigations Contains modern attacks network traces multi-class and binary classes.	It includes some biased features such as host IP, destination IP, and Date identified may create biases and not be helpful to detect the attacks.

Table 3 summarizes the popularity of various datasets, citations based on statistical comparison, and benefits and drawbacks of various benchmark datasets. The KDD Cup'99 dataset has been the most mentioned benchmark dataset since 2010, as Table 3 demonstrates. It shows that the KDD Cup'99 was utilized as a benchmark dataset for the most effort, in contrast to the other datasets. NSL-KDD is the second most referenced dataset, according to Table 3. Another benchmark dataset is the UNSW-NB15 dataset, which was created for the Australian Centre for Cyber Security [40] and contains more recent hazards. This dataset covers nine different types of attacks and consists of a training set of 175 thousand records and a testing set of 82 thousand records.

The Spanish Research National Council, or CSIC (Consejo Superior de Investigaciones Cientficas), commissioned the development of the hypertext transfer protocol (HTTP)-based dataset in 2010 to report on the criticisms of KDD'99. The dataset contains 36,600 "regular" questions and over 25,000 aberrant requests. Although these datasets are less well-known than the NSL-KDD and KDD Cup'99 databases, they may be more appropriate in some circumstances. The NSL-KDD and KDD Cup'99 are helpful benchmark datasets. Figure 3 displays the distribution of different datasets by year. The KDD Cup'99 dataset is the most popular, according to this graph, followed by the NSL-KDD dataset from 2010 to 2020. In the interim, two helpful benchmark datasets were created: KDD Cup'99 and NSL-KDD.

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

6. Approaches used in NIDS models

Liu and Lang [21] and Jyothsna et al. [22] claim that three branches of classic intrusion detection problem-solving methodologies—statistical, knowledge-based, and machine learning-based—as well as their applicable approaches were available.

Table 4: Publications of different methodologies for NIDS models

Methodology	Description	No. of Publications
Statistical Based	Well defined behaviour	185
Knowledge-based	Prior knowledge availability	126
Machine-learning based	Pattern categories	588

Table 4 shows the overall number of publications, the most citations in journals and conferences, and the intrusion detection methods. We looked at research published between 2010 and 2020. Numerous optimization methods can be used to determine the ideal intrusion detection rating. Tables 5 through 8 show different optimization methods, approaches, citations, and published paper records for intrusion detection models.

Fig. 4 displays the most widely used machine learning methods for intrusion detection. Fig. 4 compares citations to articles written by various authors and published in conferences and journals, illustrating three approaches: statistical, knowledge-based, and bioinspired. It also displays the most referenced conference articles, which were cited more frequently than journal articles.

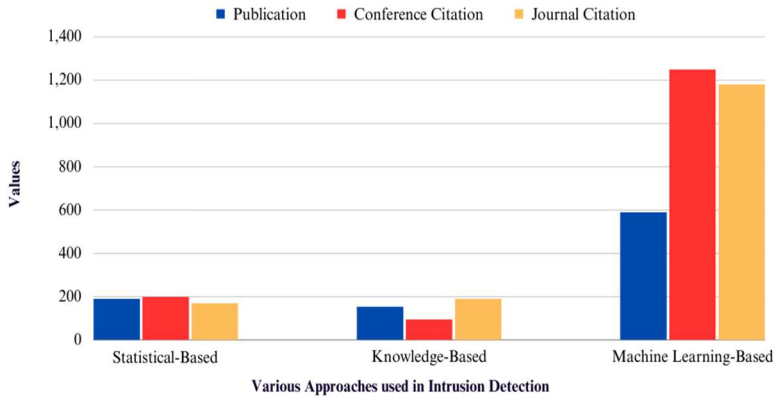

Fig 4. The total number of publications, the highest citation in conferences, and the journals for the different approaches of intrusion detection systems between the years 2010 to 2020.

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

A. Statistical-based NIDS

A statistical-based intrusion detection system (SBIDS) statistically analyzes a number of variables, including timers, resource overflow flags, and log-in sessions. The degree to which network traffic flow deviates from "normal" behavior is determined using features such as mean, standard deviation, correlation, Analysis of Variance (ANOVA), and statistical tests.

Figure 5 shows that articles about intrusion detection using a time-series statistical strategy had the most publications and the greatest citation values among all statistical approaches. Figures 6 and 7 present year-by-year comparisons of article publishing and citation patterns using various statistical techniques. Figure 5 shows that the time-series model-based IDS articles have more publications and citations than the other statistical techniques.

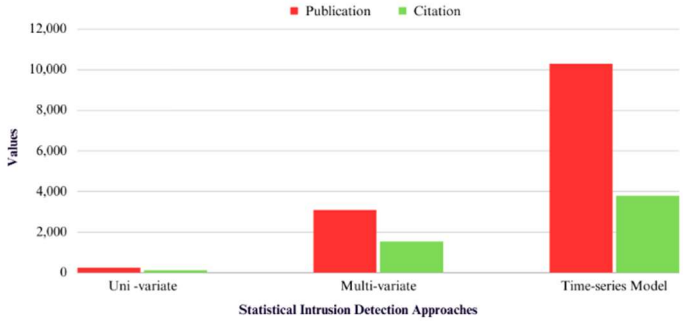

Fig 5. Various statistical-based Intrusion detection approaches with the number of publications and the highest citation in conferences and the journal between the years 2010 to 2020.

Table 5: Publications of different statistical approaches

Approaches	Total Publications	Conference Publications	Journal Publications
Time Series	10414	94	88
Multivariate	2972	64	25
Univariate	618	0	81

Here, two different points are visible. One distinction is that compared to the other statistical approaches, time series-based article publishing has a greater count. 2019 had the most publications, with 36, according to a year-by-year publishing analysis of different statistical approaches and articles based on time series model-based intrusion detection.

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

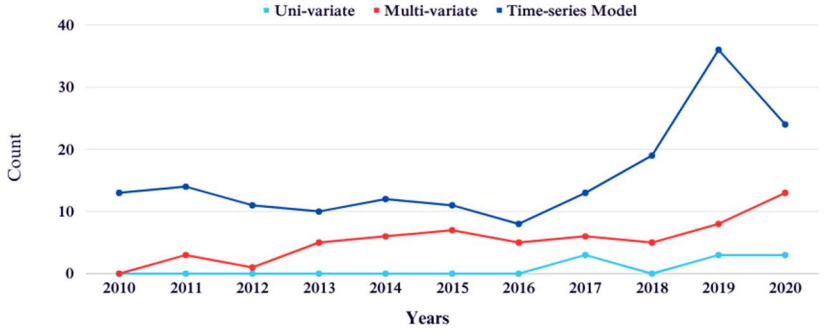

Fig 6. Year-wise articles publication distribution for statistical approaches from the year 2010 to 2020.

B. KNOWLEDGE-BASED NIDS

Knowledge-based intrusion detection systems (KBIDS) gather intrusive network data and provide low false alarm rates and high intrusion detection accuracy. However, KBIDS requires an up-to-date knowledge of network traffic behavior [23]. Table 6 lists each knowledge-based strategy's total number of publications and citations. The expert system indicates that Patcha and Park [24] have the highest number of citations (1695).

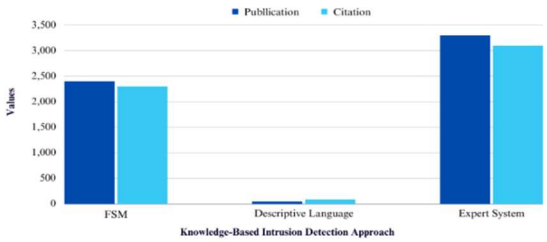

Fig 7. Publications versus citations among various knowledge-based approaches used in the intrusion detection system.

Figure 7 shows that expert system-based publication count and citations outperform both descriptive language and finite state machine (FSM). Figure 8 illustrates that between 2010 and 2020, the FSM strategy had more published publications than other knowledge-based techniques. The FSM approach's publication count for knowledge-based research papers reached its highest point in 2010 with a score of thirty. However, the total number of published articles based on the expert system is 3313, which is the biggest number of research publications in knowledge-based intrusion detection.

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

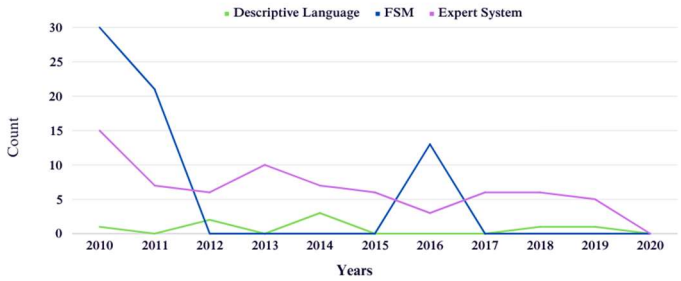

Fig 8. Publication analysis for different knowledge-based approaches along with intrusion detection.

According to the three curves in Figure 8, expert system-based articles received more citations from 2010 to 2020. This indicates that the study trend in the expert system approach to knowledge-based intrusion detection outperforms the other knowledge-based techniques.

C. MACHINE LEARNING-BASED NIDS

NIDS development has always been based on high-dimensional network traffic classification into normal and invasive data. Traditional NIDS detects unwanted content significantly more slowly due to the large dimensionality of network traffic data. Traditional NIDSs that use a machine learning technique on particular attributes have a low false-positive rate (FPR) and a high true-positive rate (TPR) when it comes to forecasting network traffic behavior [25]. Machine learning-based classifier models were developed and fitted on training sets using specific "critical" features. The 'important' and pertinent feature subsets are used to train the machine learning-based classifier.

The SVM is one of the most used techniques among intrusion detection researchers, as shown in the above table. Two attractive machine learning-based intrusion detection systems are decision trees and neural networks. Table 6 also shows the overall number of publications and the most often cited articles from journals or conferences.

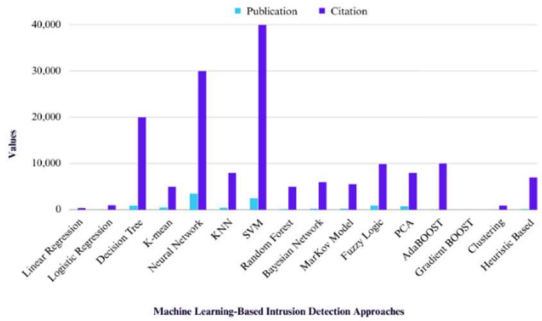

Fig 9. Publications versus citations among several Machine learning approaches implemented for intrusion detection

According to the poll, the most frequently discussed topic is publications based on SVM for intrusion detection systems. Neural-network-based intrusion detection is ranked higher than SVM and fuzzy logic in published studies, as Figure 11 illustrates. Gao et al. [26], however, addressed the limitations of the SVM technique, which is sluggish and produces little accuracy increase. The AdaBoost-based model is not perfect, and the logistic regression technique's intrusion detection accuracy is not very high.

Table 6 : Machine Learning-based IDS

Approaches	Total Publications	Conference Publications	Journal Publications
SVM	1725	128	190
Neural Network	2212	795	823
Decision Tree	763	311	745
Fuzzy Logic	823	58	110
KNN	252	125	265
PCA	381	125	184
Hueristic-Based	217	208	255
Bayesian Network	229	9	748
MarKov Model	284	92	194
Random Forest	121	241	305
K-Mean	297	120	265
AdaBOOST	111	424	133
Logistic Regression	90	78	102
Linear Regression	28	13	0
Clustering	15	32	10
Gradient BOOST	1	3	0

7. Performance measurements

By examining its effectiveness and efficiency, network security performance may be evaluated. Efficiency is all about the resources that must be allotted to the system, like primary memory and CPU cycles. Conversely, efficacy is the system's capacity to discriminate between intrusive and non-intrusive actions. In the context of IDS assessment, researchers typically utilize metrics to assess the effectiveness of the classifier based on training and testing on benchmark datasets. Unlike normal circumstances, these metrics assess the effectiveness of attack instance detection. The receiver operating characteristic (ROC) curve and the confusion matrix are the main tools used to determine how successful the IDS is.

The ROC curve and confusion matrix have a total of 54 and 2045 publications, respectively. To select

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

publications, combine the search terms in Table 1 with the filters listed in Section III. Figure 10 illustrates the relationship between citation and publication counts in the intrusion detection field for confusion and ROC. The confusion matrix is gaining popularity and has strong research trends in intrusion detection for evaluating IDS models, as this graphic shows.

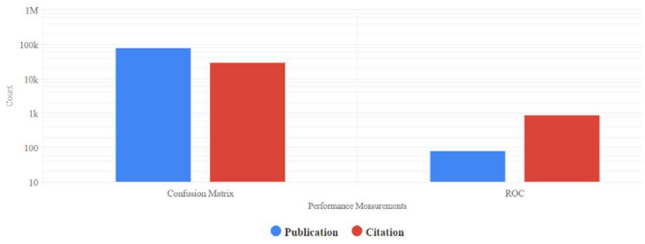

Fig 10: Confusion matrix and ROC evaluation

A. Confusion Matrix

The results obtained by an IDS are characterized and classified by using a confusion matrix. There are several different metrics for measuring fundamental parameters of the confusion matrix.

		Predicted Class	
		0	1
True Class	0	TN	FP
	1	FN	TP

Fig 11: Confusion Matrix

The basic parameters are:

- TP : True Positive (classified as normal)
- FP: False Positive (wrongly classified as normal)
- TN: True Negative (classified as attack)
- FN: False Negative (wrongly classified as attack)

1. **Misclassification Rate :** MCR tells how often a wrong classification occurs

$$\boldsymbol{MCR = \frac{FP + FN}{TP + TN + FP + FN}}$$

2. **Accuracy:** Defines how often the classifier is correct

$$\boldsymbol{Accuracy = \frac{TP + TN}{TP + TN + FP + FN} X100(\%)}$$

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 3, April 2026
PP 1–22

3. **True Positive:** Defines total no. of correct classification regarding incorrect classifications. It is also known as recall

$$\boldsymbol{TruePositive\ Rate} = \frac{\mathbf{TP}}{\boldsymbol{TP + FN}}$$

4. **Specificity:** Defines how correctly the classifier identifies true negatives. Also known as Truen Negative Rate

$$\boldsymbol{SPecificity} = \frac{\mathbf{TN}}{\boldsymbol{TN + FP}}$$

5. **Precision:** How often, normal classification is correct

$$\boldsymbol{Precision} = \frac{\mathbf{TP}}{\boldsymbol{TP + FP}}$$

6. **False Positive Rate:** How often attacks are predicted as normal

$$\boldsymbol{FPR} = \frac{\mathbf{FP}}{\boldsymbol{TP + FN}}$$

7. **Prevalence:** How often 'yes' condition actually occurs in the sample.

$$\boldsymbol{Prevalence} = \frac{\mathbf{TP + FN}}{\boldsymbol{TP + TN + FP + FN}}$$

8. **F-Score:** It is a form of derived effectiveness measurement.

$$\boldsymbol{F - Score} = \frac{\mathbf{2 * TP}}{\boldsymbol{2 * TP + FP + FN}}$$

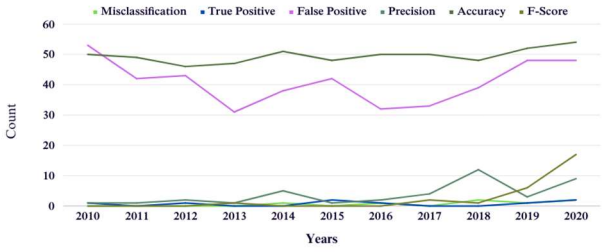

Fig 12: Publication Distribution of Evaluation metrics in IDS

B. ROC (Receiver Operating Characteristics)

The ROC curve is another way to assess an IDS's efficacy and efficiency. A performance curve and a ROC are comparable. The ratio of false alarm rate to detection accuracy is displayed by the ROC curve. Additionally, it displays the detector's false alert rate for a certain detection probability. The classification error in an IDS is computed using the area under the curve (AUC). The intrusion detection model's

performance is risky and the rate of misclassification is more than 50% if the AUC is less than or equal to 0.5. Figure 13 shows the distribution of publications by year. This chart shows that the popularity and research trend in intrusion detection using ROC to assess the IDS model is extremely modest in terms of accuracy, specificity, and FPR. Since 2010, the quantity of articles concerning ROC in the intrusion detection sector has been steadily increasing.

Fig 13: Publication distribution for roc for evaluation of IDS

8. Conclusion

This paper has studied the many kinds of intrusion detection systems, intrusion detection techniques proposed in the literature, and intrusion detection algorithms. This review was based on a number of scholarly papers. Between 2010 and 2020, a large number of publications and articles were published. In this study, we used citation as a quantitative metric to assess the intrusion detection system's popularity in comparison to other methods. This article includes a number of tables that provide a quick overview of various NIDS, research trends, and study focus. A graphic depiction of the comparative research trend analysis for intrusion detection systems for a network is also given, based on the number of published articles. We have found that while signature-based methods offer high detection accuracy for existing attacks, they cannot detect new attacks since their signatures are missing from the database. We also found that they are susceptible to zero-day attacks for the same reason. However, even though anomaly-based techniques are quite accurate at detecting and labeling unknown attacks, they have a high false alarm rate. We also examined many approaches for classifying the alerts produced by anomaly-based techniques. Finally, we examined a few hybrid approaches to intrusion detection systems (IDS) that integrated many methodologies and found that this improved intrusion detection accuracy and total detection rate. Finally, we also identified some of the suggested IDS in the literature and their possible future uses.

9. References

[1] M. Bishop, ‘‘Trends in academic research: Vulnerabilities analysis and intrusion detection,’’ Comput. Secur., vol. 21, no. 7, pp. 609–612, Nov. 2002.
[2] Kumar, Sangwan. Signature Based Intrusion Detection System Using SNORT.

[3] M. Zamani and M. Movahedi, ‘‘Machine learning techniques for intrusion detection,’’ 2013, arXiv:1312.2177.
[4]Yang, McLaughlin et al. Stateful Intrusion Detection for IEC 60870-5-104 SCADA Security.
[5]S. Agrawal and J. Agrawal, ‘‘Survey on anomaly detection using data mining techniques,’’ Proc. Comput. Sci., vol. 60, no. 1, pp. 708–713, 2015.
[6]D. Camacho, ‘‘Bio-inspired clustering: Basic features and future trends in the era of big data,’’ in Proc. IEEE 2nd Int. Conf. Cybern. (CYBCONF), Jun. 2015, pp. 1–6.
[7]M. Ahmed, A. N. Mahmood, and J. Hu, ‘‘A survey of network anomaly detection techniques,’’ J. Netw. Comput. Appl., vol. 60, pp. 19–31, Jan. 2016.
[8]A. A. Gendreau and M. Moorman, ‘‘Survey of intrusion detection systems towards an end-to-end secure Internet of Things,’’ in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud), Aug. 2016, pp. 84–90.
[9]Y. Hamid, Balasaraswathi, V. Ranganathan, L. Journaux, and M. Sugumaran, ‘‘Benchmark datasets for network intrusion detection: A review,’’ Int. J. Netw. Secur., vol. 20, no. 4, pp. 645–654, 2018.
[10]P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, ‘‘A detailed investigation and analysis of using machine learning techniques for intru-sion detection,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 686–728, 1st Quart., 2019.
[11]Qassim, Zin et al. Anomalies Classification Approach for Network-based Intrusion Detection System.
[12]J. P. Anderson, ‘‘Information security in a multi-user computer envi-ronment,’’ in Advances in Computers, vol. 12. Amsterdam, The Nether-lands: Elsevier, 1972, pp. 1–36.
[13]R. Zuech, T. Khoshgoftaar, and R. Wald, ‘‘Intrusion detection and big heterogeneous data: A survey,’’ J. Big Data, vol. 2, no. 3, pp. 1–41, Dec. 2015
[14]C. V. Anchugam and K. Thangadurai, ‘‘Classification of network attacks and countermeasures of different attacks,’’ in Network Security Attacks and Countermeasures. Hershey, PA, USA: IGI Global, 2016, pp. 115–156.
[15]A. A. Ghorbani, W. Lu, and M. Tavallaee, ‘‘Network attacks,’’ in Network Intrusion Detection and Prevention. Boston, MA, USA: Springer, 2010, pp. 1–25.
[16]M. Pihelgas, ‘‘A comparative analysis of open-source intrusion detection systems,’’ Tallinn Univ. Technol., Univ. Tartu, Tallinn, Estonia, Tech. Rep., 2012. [Online]. Available: http://mauno.pihelgas.eu/files/ Mauno_Pihelgas-A Comparative Analysis of Open- Source Intrusion Detection_Systems.pdf
[17] S. Patil, P. B. Rane, P. S. Kulkarni, and B. B. Meshram, ‘‘Snort, BRO, NetSTAT, emerald and SAX2: A comparison,’’ Int. J. Adv. Res. Comput. Sci., vol. 3, no. 2, pp. 317–323, 2012.
[18]V. R. Balasaraswathi, M. Sugumaran, and Y. Hamid, ‘‘Feature selection techniques for intrusion detection using non-bio-inspired and bio inspired optimization algorithms,’’ J. Commun. Inf. Netw., vol. 2, no. 4, pp. 107–119, Dec. 2017.
[19] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, ‘‘A sur vey of network-based intrusion detection data sets,’’ Comput. Secur., vol. 86, pp. 147–167, Sep. 2019.

[20] J. McHugh, ‘‘Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as per-formed by Lincoln Laboratory,’’ ACM Trans. Inf. Syst. Secur., vol. 3, no. 4, pp. 262–294, Nov. 2000.
[21] H. Liu and B. Lang, ‘‘Machine learning and deep learning methods for intrusion detection systems: A survey,’’ Appl. Sci., vol. 9, no. 20, p. 4396, Oct. 2019.
[22] V. Jyothsna, V. R. Prasad, and K. M. Prasad, ‘‘A review of anomaly-based intrusion detection systems,’’ Int. J. Comput. Appl., vol. 28, no. 7, pp. 26–35, 2011
[23] S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, ‘‘A survey on anoma-ly based host intrusion detection system,’’ J. Phys., Conf. Ser., vol. 1000, Apr. 2018, Art. no. 012049.
[24] A. Patcha and J.-M. Park, ‘‘An overview of anomaly detection tech niques: Existing solutions and latest technological trends,’’ Comput. Netw., vol. 51, no. 12, pp. 3448–3470, Aug. 2007.
[25] O. Almomani, ‘‘A feature selection model for network intrusion detec-tion system based on PSO, GWO, FFA and GA algorithms,’’ Symmetry, vol. 12, no. 6, p. 1046, Jun. 2020.
[26] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, ‘‘An adaptive ensemble machine learning model for intrusion detection,’’ IEEE Access, vol. 7, pp. 82512–82521, 2019.