Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
ISSN: 2788-7421

Survey of Intrusion Detection Using Deep Learning in the Internet of Things

Baraa I. Farhan[1,*], Ammar D. Jasim[2]

[1]Department of Information and Communication Engineering, Al-Nahrain University, Baghdad, Iraq
[2]Department of Information and Communication Engineering, Al-Nahrain University, Baghdad, Iraq

*Corresponding Author: Baraa I. Farhan

DOI: https://doi.org/10.52866/ijcsm.2022.01.01.009
Received October 2021; Accepted November 2021; Available online January 2022

ABSTRACT: The use of deep learning in various models is a powerful tool in detecting Internet of Things (IoT) attacks and identifying new types of intrusion to access a better secure network. The need to develop an intrusion detection system to detect and classify attacks in an appropriate time and automated manner increases particularly because of the use of IoT and the nature of its data that causes an increase in attacks. Malicious attacks are continuously changing, causing new attacks. In this study, we present a survey about the detection of anomalies and detect intrusion by distinguishing between normal and malicious behaviors whilst analyzing network traffic to discover new attacks. This study surveys previous research by evaluating their performance through two categories of new datasets of real traffic (i.e. CSE-CIC-IDS2018 and Bot-IoT datasets). To evaluate the performance, we show accuracy measurement for detect intrusion in different systems.

Keywords: Internet of Things (IoT); Intrusion Detection System (IDS); Deep Learning (DL); CSE-CIC-IDS2018; Bot-IoT

1. INTRODUCTION

Supervisory Control and Data Acquisitions and Industrial Control Systems are important, which the Critical National Infrastructures depend in managing its production using the Internet of Things (IoT). The national infrastructure includes electrical service providers in transmission and distribution, water and gas distributors and hospitals, which have become vulnerable to electronic attacks and security challenges. To overcome these electronic attacks and security challenges, protection has become a vital issue for securing European networks, information and electronic communications [1]. To secure the network against different forms of attacks using several defence lines, Intrusion Detection System (IDS) represents a second defence line against the different forms of attacks [2]. IDSs distinguish between normal and malicious behaviours based on specific rules that describe specific attack patterns or normal system behaviour [3]. IDS must satisfy time efficiency and high accuracy with low complexity to obtain better performance [4]. Data mining helps achieve higher accuracy to novel types of intrusion through knowledge discovery and demonstrates more robust behaviour than traditional IDSs [5]. The dataset represents an essential factor in testing the efficiency of intrusion detection mechanisms and the need for reliable datasets containing benign behaviour and various attacks [6, 7]. The future of the IoT for making life easier by integrating artificial intelligence (AI) has reformed all fields of life in general by making everything smart. Human intervention is not needed to make human life more comfortable [8]. The IoT suffers from weak network protocols and the loss of sufficiently robust mathematical analysis methods, leading to an increase in attacks [9].

Many types of research are discussed with their challenges and highlighted the robust factors in the detection of IoT attacks. Robust factors are used to evaluate these attacks by covering previous research and evaluating the model

performance of deep learning using two new datasets of real traffic (i.e. CSE-CICIDS2018 and Bot-IoT datasets). These factors are as follows: 'high accuracy rate', 'high detection rate' (DR) and 'low false alarm report' (FAR); these factors influence NIDS performance.

Our contributions in this work are the following:

- We survey previous studies of NIDS that use deep learning techniques.
- We show two new real datasets of network and IoT for intrusion detection.
- We compare the performance of different deep learning models with deferent datasets of network and IoT.

2. NETWORK IDS (NIDS

Technological development resulted from dependence on global networks when using several businesses, educational and social activities. As a result of the increasing use of computer network, several issues occurred on Internet security. Hence, keeping the security of devices connected to the Internet is important to ensure system availability and integrity [10]. Typically, network traffic is captured in packet and stream format, where network traffic is generally captured at the packet level by copying ports to network devices, and its data contains payload information. Flow-based data contain only network connection metadata [11]. Managing networks, analysing user information networks and services and discovering security vulnerabilities on time are useful tools for passive traffic collection and analysis [12]. The protection and prevent unauthorised access for the systems can achieve by using Firewalls and authentication methods. However, these methods lost the ability to monitor the network traffic, particularly in case of internal attacks by disgruntled employees who have legitimate network access, and the use the privilege to destruct [13]. Figure 1 shows the steps for providing network security.

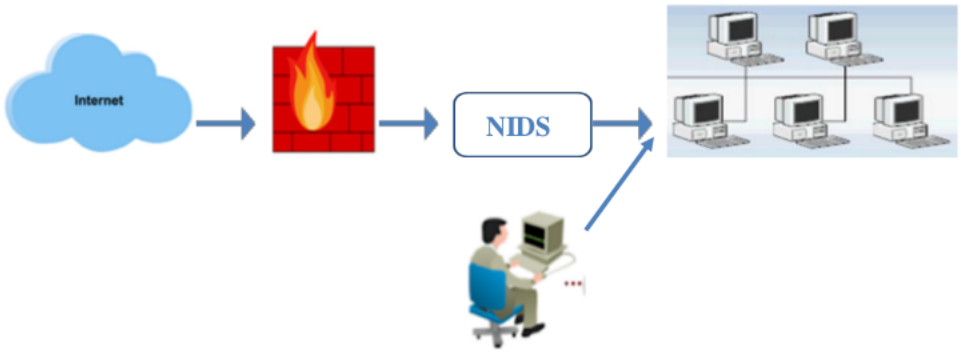

FIGURE 1. **Intrusion Detection System.**

IDSs have two different functions: intrusion alarming, which represents the first function and detects the malicious activity in the system, and the site security office SSO, which responds to the alarm and takes the appropriate action [14].

IDSs have three types, namely, 'anomaly-based detection', 'signature-based detection' and 'specification-based detection' [15]. Figure 2 depicts the categories for the IDS.

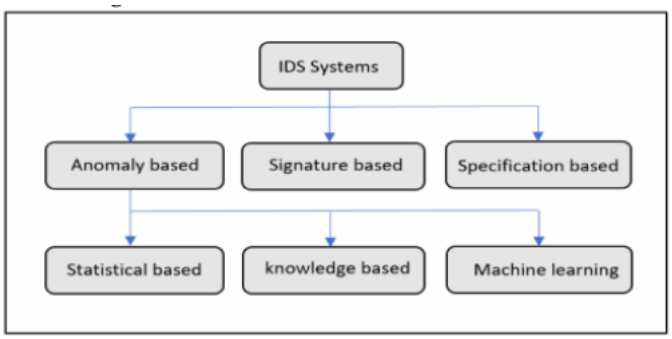

FIGURE 2. **Types of IDS systems.**

1. **'Anomaly-based detection' techniques** are dependent on the conceptualisation of a normal or legitimate profile that is obtained in the normal conditions of the network without attacks, which mostly refer to statistical data [16]. This study focused on IDS based on an anomaly. Thus, the existing sub-classification of this system is as follows:

- **'Statistical-based anomaly IDS'** periodically captures from the traffic statistical features and matches them with the normal operation of a generated stochastic model of traffic [17]. The pattern deviation between the two statistical models notifies as an attack, that is, the stored normal one and the captured one taken from the network currently..
- **Knowledge-based anomaly IDS'** Experts put many laws as an expert system or put a definition to the connection's behaviour to recognise the normal behaviour and attacks into the fuzzy-based system. The rule-based will be as inputs in this system [18] and sometimes can describe the behaviour of attacks by using heuristics or a UML.
- **'Machine learning-based anomaly IDS'** develops a model for the analysed patterns, which is explicit or implicit. These models should be regularly updated to support the efficiency of intrusion detection based on past results [19].

2. Signature-Based Technique

This type is known as misuse or knowledge-based detection, which matches the signature of the attack with the current traffic. If a matching is found, then there is a report about an attack; otherwise, no attack exists. This approach is distinguished from other approaches because it has a low false alarm rate and must update the signature continuously [20].

3. Specification-Based Technique

This type depends on matching the predetermined and memorised specification with the criteria or specification to detect a certain programme's operation and notify any violation of such criteria [21].

This study focuses on anomaly-based NIDS, which is considered because it helps detect new threats in IoT. The NIDS analyses the network traffic and detects new and unknown attacks. The feature set design is important to identify network traffic, and it is an ongoing research problem [22].

3. TECHNIQUES TO DESIGN NIDS

These techniques show general algorithms to design efficient NIDS based on AI, describing the most algorithms used in Machine Learning Techniques (ML) and Deep Learning Techniques (DL). The classification depends on types of algorithms, which include supervised and unsupervised algorithms [23]. Supervised algorithms refer to the user information that is extracted from the known and labelled data. In comparison, unsupervised algorithms extract beneficial information and features from unlabelled data. The most famous examples of ML include Decision Tree (DT), Support Vector Machine (SVM), Bayesian Algorithm, K-Nearest Neighbor and Principal Component Analysis (PCA). In addition, examples of DL are Auto Encoder (AE), Variant Auto Encoder (VAE), Deep Belief Networks (DBN), 'Convolutional neural network' (CNN), 'Recurrent neural network' (RNN), 'Long Short Term RNN' (LSTM), 'Bi-directional RNN' (BRNN), Gated Recurrent Units (GRU) and Generative Adversarial Network (GAN)), including other NIDS techniques.

3.1 ML

ML is a branch of AI that enables machines to learn helpful information extracted from big datasets automatically. Using the techniques of intelligence with the IoT devices and networks manages many security problems. Some of the recent ML/DL techniques with IoT were reviewed from a security point of view [24]. The challenges of Intrusion Detection that face big data led to providing feature selection with high classification efficiency, and this selection is reduced computational costs [25]. Hidden Markov Models (HMM), one of the statistical machine learning methods in [26], developed a database of HMM templates and two architectures that can detect and track the progress of attacks in real time, which presented diverse performance. The DT classifier has applied the 'Feature grouping based on linear correlation coefficient' (FGLCC) algorithm and 'cuttlefish algorithm' (CFA) [27]. The dimensionality reduction technique was integrated with the 'information gain' (IG) method and PCA, intrusion detection by a hybrid approach that results in merging the two algorithms [28].

3.2 DL

DL is an artificial neural network with multi-hidden layers that represent a subset of the ML. DL is more efficient and accurate than ML in many domains, such as object detection, language translation and speech recognition. Its structure is deep and has the self-ability to learn from the dataset to generate the output based on essential features. Recent studies are reviewed, and the DL approaches are used to propose solutions of NIDS. ML has the ability to self-learn from data without the need for human knowledge and coded command's ability to self-learn from data without the need for human's knowledge or coded commands. Hence, ML could understand from raw data, such as text, making it different from DL, whereas DL is provided with more data, which predictive accuracy is increased [29].

Deep learning is an essential support for enhancing IDS performance that provides the associated definitions for IDS, clarification for different IDS types and its uses [30]. The sparse auto-encoder and softmax regression have been used in NIDS to evaluate anomaly detection accuracy using benchmark network intrusion dataset NSL-KDD [31]. Software-Defined Network (SDN) showed potential to make a strong secured network, made a dangerous increase in attacks chances and also made a serious increase in attacks chances, with the clarification of potential of using DL for anomaly detection system based on the flow [32]. A survey about IoT architecture has presented emerging security vulnerabilities in the layers of the IoT architecture [33].

Dealing with big data is a challenge for IDS, but deep learning with its ability to handle big data helps meet this challenge. Deep learning has the ability to extract features automatically without the need for features engineering, compared with machine learning [34]. Therefore, deep learning feasibility in network traffic analysis has been shown and also discussed in the recent work of DL with network anomaly detection [35]. Some IDSs which adopted deep learning approaches executed in intrusion detection showed limitations, advantages and disadvantages [36–39]. A hybrid model is proposed to consist of RNN with 'Restricted Boltzmann Machines' (RBM). This hybrid model does malicious traffic detection through classification task without feature engineering [40].

The intrusion detection method suggested based on CNN to execute complex features automatically in continually changing environments, which is considered essential in network intrusions detection [41]. DNN-IDS showed more communicative and improved user trust because the black-box nature of DNNs inhibits translucence of the DNN-IDS, which is primary for building trust. The user depicted input features that are most relevant in detecting every type of intrusion by training DNN-IDS [42].

The 'hierarchical spatial-temporal features-based IDS' (HAST-IDS) described a new IDS. Firstly, HAST-IDS represented spatial features by the traffic of network in low-level which learned using deep CNNs and then, temporal features in high-level are learned using LSTM [43]. Many deep learning approaches have been used for IDS, and the accuracy and precision of three models, namely, a 'vanilla deep neural net' (DNN), 'Self-Taught Learning' (STL) approach and RNN-based LSTM, are evaluated [44]. A new deep learning system proposed a design within the youth network for detecting attacks using 'Bi-directional LSTM RNN' (BLSTM RNN) [45]. The structure of DBN's network optimised by proposing a new structure includes the design of 'Particle Swarm Optimisation' (PSO) by using learning factor and adaptive inertia weight. Then, the PSO is developed by using the fish swarm behaviour [46]. The proposed system used the Deep Learning technique, which used a combination fusion of 'Random Forest' (RF) Algorithm and DT Classifiers and detected attacks with better accuracy and reduced irrelevant features [47].

The hybrid framework of DNN called 'Scale-Hybrid-IDS-Alert Net' (SHIA) has been proposed, which monitors the traffic of the network in real time and events at the host-level effectively. This SHIA is alert to probable cyber-attacks [48]. A novel AE-based deep neural network architecture elicits related knowledge of the expected relations between the major features (spatial-features) and their timely evolution (temporal-features), where multiple autoencoders have embedded with convolutional and RNNs [49]. Deep CNN has suggested a new system by using 'deep-convolutional-neural network-based' and obtaining stable traffic characteristics, identifying the browser using nonlinear multiclass classification algorithms [50, 51].

To exceed the challenges resulting from multi tunnels of traffic, a method of source identification is suggested to identify the multiple sources of video in one encrypted tunnel using DL [52]. The proposed method depends on an image that classifies encrypted traffic of the network with high accuracy, which converts the first few non-zero payload sizes of the session into grayscale images and classifies the converted grayscale images to perform the aim from encrypted network traffic classification by using CNNs [53]. Figure 3 shows the classification of DL used for attack detection.

3.3 OTHER (NIDS) TECHNIQUES

Other techniques such as swarm intelligence, genetic algorithm and data mining are used for designing NIDS. Research on these topics is described in this section.

Strong methods for efficiently detecting and identifying data flow are configured by combining data mining techniques with Swarm intelligence. After, networks of IoT have been secured through authentication and encryption, but they suffer from poor security versus cyber-attacks. Thus, detection methods based on anomaly is used to decrease the risk of attacks types [54]. The feature selection method used the firefly algorithm, delivers the resulted features to the classifier and then provided C4.5 and 'Bayesian Networks' (BN) for attack classification [55]. The intrusion detection model designed based on 'Deep Belief Network' DBN improved by Genetic Algorithm into multiple iterations of the GA faced diverse types of attacks [56]. The suggested method used the fuzzy aggregation method with the DBNs, and 'modified density peak clustering algorithm' (MDPCA) is divided the training set into diverse subsets to reduce the size and imbalanced samples, which have similar sets of attributes [57]. The hybrid method based on anomaly screening to IDS by using 'AdaBoost

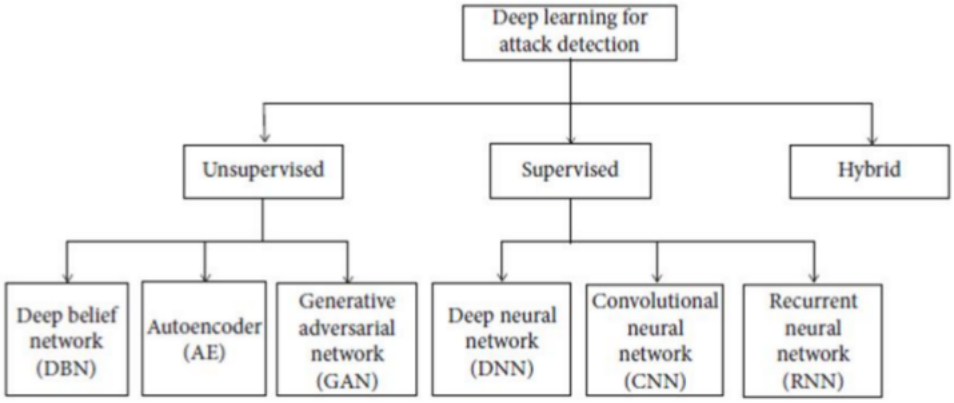

FIGURE 3. General Classification of Deep Learning

algorithms' with 'Artificial Bee Colony' (ABC) has shown a little 'false positive rate' (FPR) with a large 'detection rate' (DR) [58].

4. IDS AND IOT

In this section, the IDS research for IoT is presented. Moreover, a model for distributed attack detection framework for IoT based on semi-supervised Fuzzy learning is proposed [59]. A group of IDSs suggested detecting abnormal actions using methods based on the AdaBoost as a learning method. This group of IDSs was used to detect special botnet attacks versus 'Domain Name System' (DNS), 'Hypertext Transfer Protocol' (HTTP) and 'Message Queue Telemetry Transport' (MQTT) [60]. To detect a new attack, a group 'Hybrid IDS' (HIDS) is used, which uses a C5 as a classifier for detecting well-known intrusion and C5 as a classifier for detecting well-known intrusion and SVM classifier with One-Class [61].

The comprehensive study focused on highlighting taking trade-off accuracy and performance overheads to achieve an effective intrusion detection of the trade-off between detestation for IoT [62]. The proposed model used DL to perform efficient detection of IoT botnets. The anomalous behaviour discovered referred to botnet attacks in network traffic with a network-based method performing techniques for deep packet checking [63]. The model of a specification-based IoT intrusion detection suggested protecting against unknown attacks, which has achieved protection against previously unknown and attacks higher accuracy detection in addition efficient performance (memory and communication overhead) [64]. An innovative approach is proposed using blockchain technology for intrusion detection for IoT. The approach comprises local agents and a central component that coordinates information (alerts) received from these agents [65].

A deep learning-based method has been used in the physical layer attacks detection in IoT networks. Particularly, this study highlights attacks where an attacker tries to embody a victim IoT device into the trace of Radio Frequency (RF) [66]. An analytic study for IDSs depends on three factors: cost of computation, privacy and energy consumption [67]. A new IDS is suggested, which used machine learning algorithms for detecting anomalies in IoT. Simplification of the collaboration between protocols has been used in IoT by using the platform-provided 'security as a service' for detection [68]. Risk analysis presented and examined each layer related to the security threats. The convenient procedures and their limitations of IoT protocols are specified [69].

The new model has used PCA to reduce the dimensions from a great number of features to a small number in the dataset by using a machine learning algorithm for intrusion detection [70].

This study clarifies that current data sets (KDD99 and NSLKDD) do not give acceptable results because of three main issues: it lost the modern attack patterns, it lost modern scenarios of traffic streams and the distributed sets of training and testing are difficult. Therefore, the generated UNSW-NB15 dataset was used to address these issues [71]. The 'variant-GRU' is learned packet payloads with header features of the network automatically. 'E-GRU' and 'E-BinGRU' are new techniques never been previously used for in-network intrusion detection [72]. Figure 4 shows the typical IDS for the IoT environment.

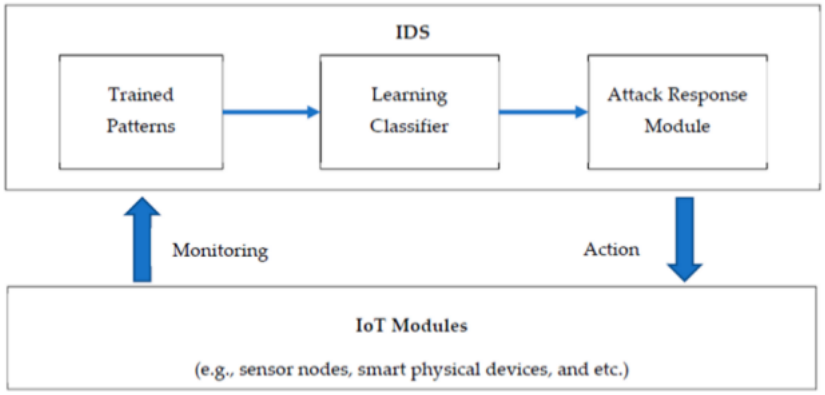

FIGURE 4. Typical intrusion detection system for IoT environment.

5. NIDS ON IOT USING DEEP LEARNING

The improvement in neural network algorithms made the application of DL more practical. The use of deep learning is considered the most flexible in detecting new attacks through its ability to extract features at a high level.

The experiments proved that the distributed attack detection system is better than centralised detection systems using a deep learning model [73]. This study has displayed some smart city problems based on home automated systems and used UCI data set possessed from temperature sensors and images of personal walkways [74]. The new detection framework is proposed by using emulation to prove its scalability and real-network traffic for proving the concept. The detection options are provided as a service and spread interoperability between IoT protocols [75]. The proposed system was created by applying AI on detected botnet attacks that are caused by increasing threats on banking services and financial sectors. This system uses IDS dataset in 2018, which is a real-time dataset (CSE-CIC-IDS2018), created by the Canadian 'Institute for Cyber Security' (CIC) on the environment of 'Amazon Web Services' (AWS) [76]. An attacks-detection system is shown by using BLSTM RNN as deep learning technology within the network [77]. The lightweight distributed security solution has shown to develop IoT architecture, analyse the approaches of ML and DL on the IoT and Cyber Security and evaluate networks (LSTM and GRU) for each layer in the architecture of the IDS dataset [78].

6. PUBLIC DATASETS

Choosing the type of database used in extracting information is of great importance as it supports the work of the model used in the detection. Several types of cyber security datasets are used for intrusion detection, which can classify into seven main categories as follows [78]: 'network traffic-based' dataset, 'electrical network-based' dataset, 'internet traffic- based' dataset, 'virtual private network-based' dataset, 'android apps-based' dataset, 'IoT traffic-based' dataset and 'internet-connected devices-based' dataset, as shown in Fig. 5 with their subtypes. This survey will focus on two new real traffic datasets: the CSE-CIC-IDS 2018 dataset and the Bot-IoT dataset. Table 1 also presents an analytical comparison of the accuracy results of the research that dealt with the use of NIDS for IoT.

6.1 NETWORK TRAFFIC-BASED DATASET (CSE-CIC-IDS2018 DATASET)

The Communications Security Establishment (CSE) and Institute for Cyber Security (CIC) built the CICIDS2018 dataset [79]. The CICIDS2018 contains seven attack types Brute-force, Heartbleed, infiltration, Web attacks, DoS, DDoS and Botnet, which are applied to a large scope of protocols and topologies of network calculated in forward and reverse mode. To the CICDS2017 dataset [80], the CIC Flow Meter is a tool that extracts 80 attributes from the generated traffic of the network [81]. This dataset contains PCAP and CSV formats. Originally, AI uses the CSV format whilst using PCAP format to summery new features [82].

6.2 IOT TRAFFIC-BASED DATASET (BOT-IOT DATASET)

The database represents the normal traffic of IoT networks with various attacks. The Bot-IoT database represents a real and ecosystem of IoT environment including Keylogging, OS, Service Scan, DDoS, DoS and Data exfiltration attacks. Koroniotis et al. [83] proposed the Bot-IoT as a new dataset for comparing IoT environments with previous datasets,

which uses the MQTT protocol as a lightweight communication protocol. The Bot-IoT dataset has more than 72,000.000 records [84].

Table 1. Comparative analysis of existing NIDS for IoT

Ref.	Method of DL	Year	Dataset	Accuracy	IoT traces	Zero-day attacks
[84]	RNN, CNN	2021	CICIDS2018	97.75%	×	✓
[85]	Siamese-NN, DNN	2021	NSL-KDD, CIDDS-001	-	×	×
[86]	LSTM, AE	2021	ISCX-UNB	97.52%	×	×
[87]	GA, Fuzzy	2021	NSL-KDD	99.96%	×	×
[88]	Correlation-based attribute -ANN	2021	NSL-KDD, UNSW-NB	-	×	×
[89]	CST-GR with Raspberry Pi	2020	Botnet, Bot-IoT	99.4%	✓	✓
[90]	K-Nearest Neighbor, Random Forest, Gradient Boosting, Adaboost, Decision Tree, and Linear Discriminant Analysis	2020	CSE-CIC-IDS2018	Show accuracy for each attack and model in this data	×	✓
[91]	Spark MLlib, Conv-AE	2020	CSE-CIC-IDS2018	98.20%	×	✓
[92]	GA, PSO, GWO, FFA	2020	UNSW-NB15	Show accuracy for each classifier	×	×
[93]	MGA-SVM-HGS-PSO-ANN	2020	NSL-KDD	99.3%	×	×
[94]	RNN, CNN	2019	CSE-CIC-IDS 2018	Show accuracy for each attack in this data	×	✓
[95]	AFSA-GA-PSO	2019	NSL-KDD	Show accuracy for each classifier	×	×
[96]	DNN	2019	KDDCup 99	-	×	×
[97]	GA, DBN	2019	NSL-KDD	99%	×	×
[98]	SNN, DCA	2020	Bot-IoT	98.73%	✓	✓
[99]	DNN, RNN, LSTM	2018	KDD, NSL-KDD	98.9%	×	×
[100]	C5 and One Class Support Vector Machine classifier	2019	Bot-IoT	99.97%	✓	✓
[101]	LSTM, AM	2019	CSE-CIC-IDS2018	96.2%	×	✓
[102]	IDS using ML	2019	CSE-CIC-IDS2018	96.0%	×	✓
[103]	DBN	2019	CSE-CIC-IDS2018	95%	×	✓

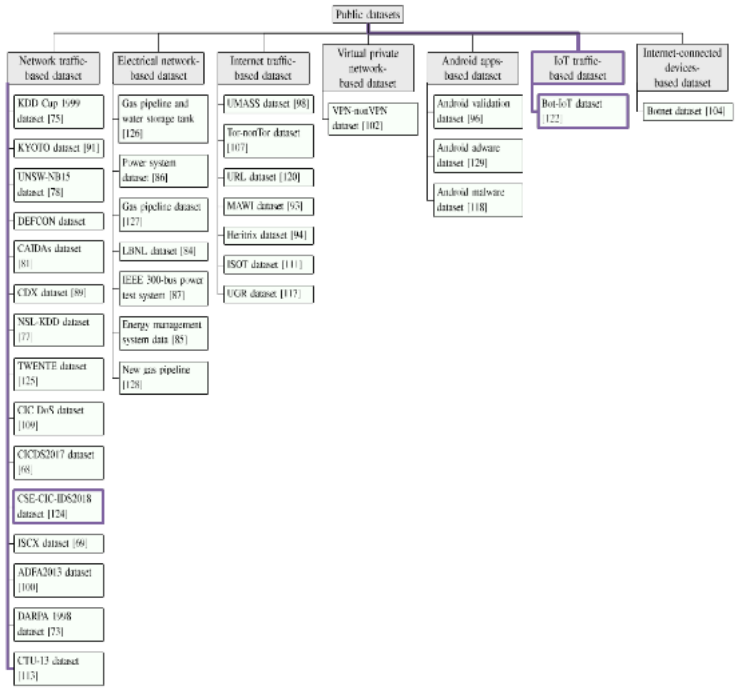

FIGURE 5. Types of Cyber Security Datasets of Intrusion Detection.

7. CONCLUSIONS

The IoT faces many challenges and security threats, and the new and various attacks exist, which negatively affect smart systems and the provision of related services. Therefore, a system should be urgently provided to detect intrusion and attacks against the network. Deep learning is more powerful than machine learning because of its ability to deal with big data and detect intrusions and new attacks, supporting the ability to self-learn and detect zero-day attacks.

This survey highlights recent studies on models of detection and integrating models to support intrusion detection and datasets. The models are applied to motivate researchers to use new datasets that include the (CSECIC-IDS2018 and the Bot-IoT) dataset as it supports the good performance of the detection model.

ACKNOWLEDGEMENTS

Special thanks to my professors at Al-Nahrain University and thanks to Wasit University. This work is not supported by any party.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] L. A. Maglaras, K. H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, and P. Fragkou.
[2] A. Ahmim, M. Derdour, and M. A. Ferrag, “An intrusion detection system based on combining probability predictions of a tree of classifiers,” *Int. J. Commun. Syst*, vol. 31, no. 9, pp. 3547–3547, 2018.
[3] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, “A novel hierarchi- cal intrusion detection system based on decision tree and rules-based mod- els,” *15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 228–261, 2019.
[4] Z. Dewa and L. A. Maglaras, “Data mining and intrusion detection systems,” *Int. J. Adv. Comput. Sci. Appl*, vol. 7, no. 1, pp. 62–71, 2016.
[5] B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, and P. Simões, “A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes,” *EAI Endorsed Trans. Ind. Netw. Intell. Syst*, no. 10, pp. 4–4, 2017.
[6] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, *Toward generating a new intru- sion detection dataset and intrusion traffic characterization*. 2018.
[7] R. Ismael, F. Abeer, T. M. Nidaa, and F, “Optimized Deep Learning with Binary PSO for Intrusion Detection on CSE-CIC-IDS2018 Dataset,” *J. Al Qadisiyah Comput. Sci. Math*, pp. 16–16, 2020.

[8] Akashshukla and A. Himanshosharma, "Future of Internet of Things: Trends, Challenges & Insight To Artificial Intelligence," *International Journal of Advanced Research in Computer*, vol. 9, no. 2, 2018.

[9] G. A. Fink, D. V. Z. Thomas, and E. Caroll, 2015.

[10] S. Q. Tan, B. H. M. Sundaram, S. Wang, T. Ng, Y. Chang, V. Aung, and K. M. M, "Secure searching on cloud storage enhanced by homomorphic indexing," *Future Gener. Comput. Syst*, vol. 65, pp. 102–110, 2016.

[11] M. H. Prasantagogoi and Bhuyan, 2012.

[12] A. A. Ghorbani, W. Lu, and M. Tavallaee, 2010.

[13] S. Ho, "Intrusion Detection - Systems for today and tomorrow," *SANS Institute 2019*, pp. 2–2.

[14] A. R. Javed, M. O. Beg, M. Asim, T. Baker, A. H. Al-Bayatti, and Alphalogger, "Detecting motion-based side-channel attack using smartphone keystrokes," *J. Ambient Intell. Humaniz. Comput*, 2020.

[15] H. Liao, C. R. Lin, Y. Lin, and K. Tung, "Journal of Network andComputer Applications Intrusion detection system," *J. Netw. Comput*, vol. 36, pp. 16–24, 2013.

[16] A. Nisioti, A. Mylonas, and V. Katos, 2018.

[17] E. Kabir, J. Hu, H. Wang, and G. Zhuo, "A novel statistical technique for intrusion detection systems," *Future Gener. Comput. Syst*, vol. 79, pp. 303–318, 2017.

[18] M. Petkovic, I. Basicevic, D. Kukolj, and M. Popovic, "Evaluation of takagi-sugeno-kang fuzzy method in entropy-based detection of DDoS attacks," *Comput. Sci. Inf. Syst*, vol. 15, pp. 139–162, 2018.

[19] A. Feizollah, S. S. Anuar, N. B. Salleh, and R, "A study of machine learning classifiers for anomaly-based mobile botnet detection," *Malaysian J Comput Sci*, vol. 26, no. 4, pp. 251–265, 2014.

[20] A. H. Hamamoto, L. F. Carvalho, L. H. Sampaio, T. Abrão, and M. L. Proença, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Syst. Appl*, vol. 92, pp. 390–402, 2018.

[21] G. Dupont, J. Hartog, S. Etalle, and A. Lekidis.

[22] Shawqm, Mehibs, H. Soukaena, and Hashim, "Proposed Network Intrusion Detection System In Cloud Environment Based on Back Propagation Neural Network," *Journal of Babylon university/Pure and Applied Sciences*, vol. 26, no. 1, 2018.

[23] M. W. Berry, M. A. Yap, and B. W, *Supervised and Unsupervised Learning for Data Science*. New York, NY: Springer, 2019.

[24] M. A. Al-Garadi, 2020.

[25] T. M. Richardzuech and Khoshgoftaar, "A survey on feature selection for intrusion detection," in *21st ISSAT International Conference on Reliability and Quality in Design*, 2015.

[26] A. Tawfeeqshawly and Elghariani, 2019.

[27] S. Mohammadi, H. Mirvaziri, and H. Mostafaghazizadeh-Ahsaee, "Cyber intrusion detection by combined feature selection algorithm," *Journal of Information Security and Applications*, vol. 44, pp. 80–88, 2019.

[28] A. Fadisalo, A. Bounassif, and Essex, "Dimensionality Reduction with IG-PCA and Ensemble Classifier for Network Intrusion Detection," *Computer Networks*, 2018.

[29] F. Gottwalt, E. Chang, T. Dillon, and Corrcorr, "A Feature Selection Method for Multivariate Correlation Network Anomaly Detection Techniques," *Computers&security*.

[30] M. Kwangjokim and Harrychaandra, "Network Intrusion Detection using Deep Learning: A Feature Learning Approach," *SpringerBriefs on Cyber Security Systems and Networks*, 2018.

[31] N. Quamar, W. Sun, Y. Ahmad, and M. Javaid, "A Deep Learning Approach for Network Intrusion Detection System," *Conference Paper in Security and Safety*, 2015.

[32] T. A. Tang, L. Mhamdi, and Mclernon, "Deep Learning Approach For Network Intrusion Detection in Software Defined Networking," *International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2016.

[33] M. F. Elrawy, A. I. Awad, F. A. Hesham, and Hame, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing :Advances, Systems and Applications*, 2018.

[34] K. Kim and Muhamaderzaaminanto, 2017.

[35] D. Kwon, Hyunjookim, S. C. Jinohkim, I. Suh, K. J. Kim, and Kim, 2017.

[36] K. Kim and Muhamaderzaaminanto, 2017.

[37] R. C. Staudemeyer, 2015.

[38] R.-H. Hwang, M.-C. Peng, V.-L. Nguyen, and Yu-Lunchang, "An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level," *AppliedScience*, pp. 9163414–9163414, 2019.

[39] G. Kim, H. Yi, J. Lee, S. Yunheungpaek, and Yoon, 2016.

[40] C. Li1, J. Wang1, and X. Ye1, "Using a Recurrent Neural Network and Restricted Boltzmann Machines for Malicious Traffic Detection," *NeuroQuantology*, vol. 16, no. 5, pp. 823–831, 2018.

[41] L. Zhang, M. Li, X. Wang, and Y. Huang, "An Improved Network Intrusion Detection Based on Deep Neural," *Network IOP Conference Series: Materials Science and Engineering*, 2019.

[42] M. Kasunamarasinghe and Manic, 2018.

[43] W. Wang, Y. Sheng, and J. Wang, "HAST-IDS: Learning Hierarchical Spatial-Temporal Features using Deep Neural Networks to Improve Intrusion Detection," *IEEE*, 2017.

[44] B. . Lee, Amaresh, . Sandhya, C. . Green, and D. Engels, "Comparative Study of Deep Learning Models for Network Intrusion Detection," *SMU Data Science Review*, vol. 1, no. 1, 2018.

[45] D. H. B. Roy and Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," *28th international Telecommunication Network Communication Conference (ITANC)*, 2018.

[46] P. Wei, Y. Li, Z. Zhang, and T. Hu, 2019.

[47] V. Kanimozhi and P. Jacob, "UNSW-NB15 Dataset Feature Selection and Network Intrusion Detection using Deep Learning," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 7, no. 5S2, 2019.

[48] R. Vinayakumar, S. P. Mamounalazab, and Prabaharanp.

[49] D. G. Palmieri and F, "Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial-temporal features extraction," *Journal of Network and Computer Applications*, pp. 102890–102890, 2021.

[50] M. Aqeel, A. D. H. Alhussainy, and Jasim, "Half Gaussian-based wavelet transform for pooling layer for convolution neural network," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 19, pp. 163–172, 2021.

[51] A. Ss, S. A. Chao, and C. Cs, "Passive browser identification with multi-scale Convolutional Neural Networks," *Neurocomputing*, vol. 378, pp. 238–247, 2020.
[52] Y. Shi, D. Feng, and Y. Cheng, "A natural language-inspired multilabel video streaming source identification method based on deep neural networks," *Signal Image and Video Processing*, pp. 1–8, 2021.
[53] Y. He and W. Li, "Image-based Encrypted Traffic Classification with Convolution Neural Networks," *IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*, 2020.
[54] S. Mishra, A. Y. Rafidsagban, and Gandhi, "Swarm Intelligence in anomaly detection systems: an overview," *International Journal of Computers and Applications*, 2018.
[55] Selvakumarb and K. Muneeswaran, "Firefly algorithm based Feature Selection for Network Intrusion Detection," *Computers & Security*, 2018.
[56] Y. Zhang, P. Li, and Xinhengwang.
[57] K. Yanqingyang, Chunhuawu, and Y. Xinxinniu, "Building an Effective Intrusion Detection SystemUsing the Modified Density Peak Clustering Algorithm and Deep Belief Networks," *Applied Science*, vol. 9, 2019.
[58] Mazinim, Shirazib, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoostalgorithms," *Journal of King Saud University - Computer and Information Sciences*, 2018.
[59] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Appl Soft Comput*, vol. 72, pp. 79–89, 2018.
[60] N. Moustafa, B. Turnbull, and K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," *IEEE Internet of Things Journal*, vol. 6, pp. 4815–4830, 2019.
[61] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks," *Electronics*, vol. 8, no. 11, pp. 1210–1210, 2019.
[62] J. Arshad, M. A. Azad, and R. Amad, "Khaled Salah, Mamoun Alazab and Razi Iqbal "A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT," *Electronics*, vol. 2020, pp. 9040629–9040629.
[63] C. D. Mcdermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, 2018.
[64] V. Sharma, I. You, K. Yim, I. Chen, and J. Cho, "BRIoT: Behavior Rule Specification-Based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems," *IEEE*, vol. 7, pp. 118556–118580, 2019.
[65] D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *Int. J. Inf. Manag*, vol. 49, pp. 533–545, 2019.
[66] J. Bassey, D. Adesina, X. Li, L. Qian, A. Aved, and T. Kroecker, "Intrusion Detection for IoT Devices based on RF Fingerprinting using Deep Learning," *Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 98–104, 2019.
[67] M. A. Junaidarshad, K. Azad, W. Salah, Jie, and M. Raziiqbal, 2018.
[68] G. Shevenchawla, "Security as a Service: Real-time Intrusion Detection in Internet of Things," *ACM ISBN*, 2018.
[69] J. Tournier, F. Lesueur, F. L. Mouël, L. Guyon, and H. Ben-Hassine, 2020.
[70] S. Zhao, W. Li, T. Zia, and A. Y, "A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things," *IEEE. 15th Intl Conf on Dependable, Autonomic and Secure Computing*, 2017.
[71] J. Nourmoustafa& and Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Information Security Journal: A Global Perspective*, 2016.
[72] Y. Yiranhao and J. Sheng, 2019.
[73] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learningapproach for Internet of Things," *Future Generation Computer Systems*, 2017.
[74] N. Rakesh, "Performance analysis of anomaly detection of different IoT datasets using cloud micro services," *International Conference on Inventive Computation Technologies (ICICT)*, pp. 1–5, 2016.
[75] S. Geethapriyathamilarasu, 1977.
[76] V. Kanimozhi and T. P. Jacob, 2019.
[77] M. K. Putchala, "Deep Learning Approach For Intrusion Detection System (IDS," *The Internet Of Things (IOT) Network Using Gated Recurrent Neural Networks (GRU)*, 2017.
[78] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, pp. 102419–102419, 2020.
[79] C.-C.-I. Dataset, 2019.
[80] Cicflowmeter, 2019.
[81] C. Dataset, 2019.
[82] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic ana- lytics: Bot-IoT dataset," *Fut. Gener. Comput. Syst*, vol. 100, pp. 779–96, 2019.
[83] Bot-Iot and Dataset, 2019.
[84] M. A. Khan, 2021.
[85] P. Bedi, N. Gupta, and V. Jindal, "I-SiamIDS: An improved Siam-IDS for handling class imbalance in network-based intrusion detection systems," *Appl. Intell*, vol. 51, pp. 1133–1151, 2021.
[86] M. A. Khan and Y. Kim, "Deep Learning-Based Hybrid Intelligent Intrusion Detection System. Comput," *Mater. Contin*, vol. 68, pp. 671–687, 2021.
[87] K. P. M. Kumar, M. Saravanan, M. Thenmozhi, and K. Vijayakumar, "Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks," *Concurr. Comput, Pr. Exp*, pp. 5242–5242, 2021.
[88] I. S. Thaseen, J. S. Banu, K. Lavanya, M. R. Ghalib, and K. Abhishek, "An integrated intrusion detection system using correlation-based attribute selection and artificial neural network," *Trans. Emerg. Telecommun. Technol*, pp. 4014–4014, 2021.
[89] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai.
[90] G. Karatas, O. Demir, and O. K. Sahingoz, "Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset," *IEEE*, pp. 32150–32162, 2020.
[91] M. A. Khan and J. Kim, "Toward Developing Efficient Conv-AE-Based Intrusion Detection System Using Heterogeneous Dataset," *Electronics 2020, 9*, pp. 1771–1771.
[92] O. Almomani.

[93] S. Hosseini, B. M. H. Zade, and A. Svm, "New hybrid method for attack detection using combination of evolutionary algorithms," *Comput. Netw*, vol. 173, pp. 107168–107168, 2020.
[94] J. Kim, Y. Shin, and E. Choi, "An Intrusion Detection Model based on a Convolutional Neural Network," *J. Multimed. Inf. Syst*, vol. 6, pp. 165–172, 2019.
[95] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li, and D. Liu, "An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network," *IEEE*, vol. 7, pp. 87593–87605, 2019.
[96] V. Kumar and R, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE*, vol. 7, pp. 41525–41550, 2019.
[97] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE*, vol. 7, pp. 31711–31733, 2019.
[98] S. Aldhaheri, D. . Alghazzawi, L. Cheng, B. Alzahrani, and A. Al-Barakati, "DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System," *Appl. Sci*, vol. 2020, 1909.
[99] B. Lee, Amaresh, Sandhya, C. Green, and D. Engels, 2018.
[100] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, 1210.
[101] P. Lin, K. Ye, and C. Z. Xu, *Dynamic Network Anomaly Detection System by Using Deep Learning Techniques*. Cham, Switzerland: Springer Science and Business Media LLC, 2019.
[102] Q. Zhou and D. Pezaros, 2019.
[103] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li, and D. Liu, "An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network," *IEEE*, vol. 7, pp. 87593–87605, 2019.