A SURVEY OF MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR INTRUSION DETECTION SYSTEMS IN IOT

Tran Thanh Cong
Ho Chi Minh City University of Economics and Finance,
141 Dien Bien Phu Street, Ward 15, District Binh Thanh, Ho Chi Minh City,
congtt@uef.edu.vn

Abstract— *The Internet of Things (IoT) is one of the fastest-growing technologies in computing and has influenced several aspects of our lives. The explosion of IoT has resulted in a spike in cyber-attack incidents. In order to mitigate this challenge, it is necessary to develop robust intrusion detection systems (IDSs). Because IDSs are considered as one of the vital components for securing computing infrastructures. This study displays a survey of machine learning (ML) and deep learning (DL) approaches for IDSs. This proposal provides the following major contributions. First, we thoroughly review different types of IDSs. Second, we analyze comprehensively common ML approaches and recent advances in DL approaches which can be utilized to foster approaches of enhanced security for IDSs. Third, several different datasets and evaluation measures are indicated in this study. Based on this survey, we recognize the open challenges and future directions for IDSs in IoT.*

Keywords— *Intrusion Detection System, Machine Learning, Deep Learning.*

1. Introduction

The development of various technical fields, such as sensors, automatic identification and tracking, embedded computing, wireless communications, broadband Internet access and distributed services, has raised the potential for integrates intelligent objects into our daily activities through the Internet. The convergence of the Internet and intelligent objects that may communicate and interact with each other defines the Internet of Things (IoT). This new paradigm is recognized as one of the most important actors in the Information and Communication Technology (ICT) industry in the coming years [1]. The IoT could have 26 billion units by the year of 2020 according to Gartner Inc., Cisco Systems predicts that the IoT will generate $ 14.4 trillion due to the integration of increased revenue and lower costs for firms between 2013 and 2022 [2], [3], [4], [5].

The IoT is very popular in our routine activities. We are currently using the IoT in our homes, in hospitals, deployed externally to inspect and report environmental changes, voting and to more profitable functions. However, those benefits may come with huge risks of loss of private consulting rights and security issues [6]. It is mainly because these devices both gather personal information, such as the user's name and phone number, and can also monitor the activities of users. A concrete example of leaking personal information is that people might know when the user is in their home and what they eat for lunch. After a never-ending chain of revelations about breaches of big data, consumers have raised awareness of placing a lot of personal data in public or private clouds. This causes the combination of the Internet and real-world objects brings the threats of cybersecurity to most of our day-to-day operations. Attacks on important infrastructures, such as transportation systems and power plants, can have devastating influences on entire towns and countries [7].

Recently, a number of studies [8], [9], and [10] have researched to enhance IoT security, consisting of approaches to provide data confidentiality and authentication, access control within the IoT network, privacy and

trust among users and things, and the enforcement of security and privacy policies [4]. However, the amount of network throughput and security threat is recently increasing significantly so the study of the intrusion detection systems (IDSs) have received a variety of attention throughout the computer science area. The existing IDSs face with challenges on both capricious intrusion categories, and huge computational power [11]. It is, therefore, essential to design IDSs to deal with these challenges. The IDSs have developed for traditional network, but the existing solutions are insufficient for innovative attacks triggered by cybercriminals owing to the volume, velocity, variety, and veracity of data. It is mainly because IoT devices generate a large amount of data that travels across networks. The data traveling through the network is at risk of network attack. These types of data are often classified as big data.

In addition, machine learning (ML) and deep learning (DL) recently show advantages and there are more and more applications of ML and DL techniques in network security. In this study, we want to survey common ML and DL approaches for IDSs. The contributions are as follow:

- Review in depth different types of IDSs.
- Analyze common ML/DL approaches to enhanced security for IDSs.
- Study a variety of datasets and evaluation measures.
- Recognize the open challenges and future directions for IDSs in IoT.

2. Intrusion Detection Systems

The IDSs have a crucial role in achieving network security. The primary goal of the IDS is to track and monitor the malicious activities of the system or the networks. The IDS can be divided into several different categories. First, it is possible to separate the IDS into active IDS and passive IDS. The function of the active IDS is to automatically block the malware attacks without any human intervention, while the purpose of the passive IDS is to alert the users and to monitor the network traffic.

Secondly, the IDS can be categorized as signature-based IDS and anomaly-based IDS in several circumstances. In the signature-based approach, the IDS accesses to a database of known signatures and security holes. Each intrusion attack includes the full details of the attack known as a signature. This attack is also utilized to identify and restrict attacks in the future. Conversely, the notable disadvantage of this approach shows that it is necessary to frequently update the database, whereas the anomaly-based IDS or behavior-based learns from the sample bases to identify new intrusion attacks. Any deviation from the sample bases is identified as an attack and warning tool is triggered [7].

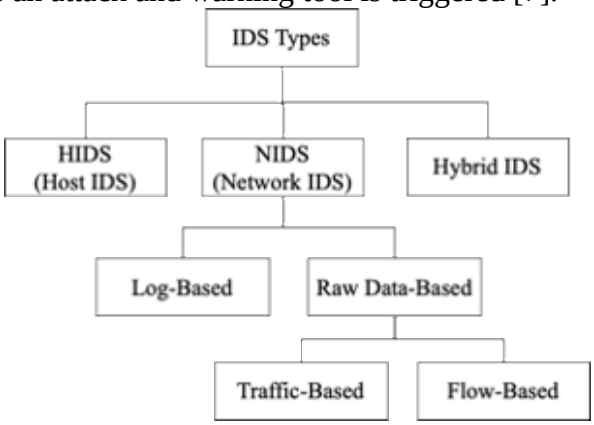

Fig. 1 Types of instruction detection system

Thirdly, another division of the IDS relies on the location where it is mounted. There are three fundamental types, known as host IDS, network IDS, and hybrid IDS [12], as shown in Fig. 1. After critical research, the NIDS hierarchy is categorized as log-based and raw data-based. Log-based NIDS evaluates logs recorded through security equipment when packets flow, whereas raw data-based NIDS contains traffic-based, and flow-base analyzes the data sent itself. The traffic-based consists of the whole packets' data, headers, and bodies, but flow-based covers only headers of packets.

3. Review machine learning and deep learing for IDSs

3.1 Machine learning for IDSs

Recently, the ML algorithms are applied to create the IDSs in IoT based on the available datasets. Table 1 summarizes various ML

approaches which are used to detect attacks in IoT. These studies generally created the reliable IDS and probably applied in some domains. However, there are several constraints in these papers. First, the accuracy of these proposed models is needed to improve in the future. Second, these studies sometimes do not work effectively in several cases as well as do not classify complex and more sophisticated attacks. Third, feature selection is still not applied to increase the performance of the models in some studies.

Table 1 Machine learning approaches for IDSs in IoT

Studies	ML approaches	Datasets	Limitations
[13]	- Random forest - Neural network	UNSW-NB15 (49 features)	- This study did not study IoT network traffic features.
[14]	- Logistic Regression - Gaussian Naïve Bayes - k-Nearest Neighbours - Support Vector Machine - Decision Trees - Random Forests	MQTT-IoT-IDS2020 (3 features)	- The accuracy of the classifiers can still improve.
[15]	- I Bayes - Bayesian Network - J48 - Zero R - One R - Simple Logistic - Support Vector Machine - Multi-Layer Perceptron - Random Forest	Private dataset	- The proposed models in this study need to further expand for more complex and more sophisticated attacks. -Feature selection should apply to seek important features for classification to increase the accuracy.
[16]	- Inverse Weight Clustering (IWC) - Decision Tree	Intel Lab Project dataset	- The model did not work effectively in some circumstances. - The accuracy of the proposed model needs to improve through finding the optimal clusters when implementing IWC. - The classifier did not use the latest version of the classifier to build the model.
[17]	- Random Forest - AdaBoost - Gradient Boosted Machine - Extreme Gradient Boosting - Extremely Randomized Trees - Classification and Regression Trees - Multi-layer Perceptron	- CIDDS-001 (12 features) - UNSW-NB15 (49 features) - NSL-KDD (41 features)	- This study did not design the IDS to defend against routing attacks in IoT networks.

3.2 Deep learning methods for IDSs in IoT

The DL which is a portion of the ML area is also investigated to establish the IDS models in IoT. Several DL algorithms described in Table 2 have been employed as the classifiers for many types of attacks. Conversely, limitations also exist in these studies. The first constraint is training time, so it is necessary to optimize the parameters to reduce the training time. The second one is that the accuracy of these proposed models needs to improve in future research. Next, the models developed in these studies mentioned in Table 2 do not work well for adversarial attacks. Ultimately, with the development of modern attacks, these models are not suited to these types of attacks.

Table 2 Deep learning approaches for IDS in IoT

Studies	DL approaches	Datasets	Limitations
[18]	- Improved genetic algorithm (GA) - Deep belief network (DBN)	NSL-KDD	The parameters of the deep network need to optimize to mitigate the training time and improve the detection accuracy.
[19]	- Feed-forward Neural Networks (FNN) - Self-normalizing Neural Network (SNN)	BoT-IoT	The outcomes indicated that feature normalization of the IoT dataset has a negative impact on the adversarial resilience of the DL based IDSs. When the input features are normalized, both IDSs based on FNN and SNN have better performance metrics, but they were easily vulnerable to adversarial samples.
[20]	- Deep Neural Network (DNN)	Private dataset	Future work includes extending the proposed IDSs to detect other types of attacks against the IoT including location dependent attacks such as cloning of device ID, spoofing, and sybil attacks.
[21]	- Deep auto-encoder - Deep feedforward neural network	NSL-KDD and UNSW-NB15	In future, this study extends this work to train this algorithm on real data collected from IoT systems to demonstrate the efficiency of its implementation.
[22]	- Multi-convolutional neural network (multi-CNN)	NSL-KDD	The further research is directed towards deep learning fusion and online learning for the network intrusion detection problem, which can protect the data of industrial IoT intelligently.
[23]	- Artificial Neural Network (ANN)	Private dataset	For future developments, more attacks shall be introduced to test the reliability of our method against attacks and improve the accuracy of the framework.
[24]	- Bidirectional Long Short-Term Memory based - Recurrent Neural Network (BLSTM-RNN)	Private dataset	The ways to improve situational awareness of botnet activity within the IoT need to investigate in future.
[25]	Improved Long Short-Term Memory (I-LSTM)	Private dataset	The detection performance in this study will improve through optimizing concept drift adaptive method. Multi-classification method needs to investigate more.

4. Review Datasets

In this research, we review several datasets and types of attacks of each dataset as shown in Table 3. The description of the datasets is described in the following subsections.

Table 3 Summary of datasets

Datasets	Types of attacks
DARPA dataset	Normal, DoS, Probe, R2L, U2R
KDD Cup 1999 dataset	Normal, DoS, Probe, R2L, U2R
NSL-KDD dataset	Normal, DoS, Probe, R2L, U2R
UNSW-NB15 dataset	Normal, DoS, Fuzzers, Analysis, Backdoors, Exploits, Generic, Reconnaissance, Shell code, Worms
KYOTO dataset	Normal, Exploits, Shell code, Malware
CICDS2017 dataset	Normal, DoS, Web, Botnet, DDoS, BruteForce
CIDDS- 001 dataset	Normal, DoS, PortScan, BruteForce, PingScan
CSE-CIC-IDS2018 dataset	Bruteforce attack, DoS attack, Web attack, Infiltration attack, Botnet attack, DDoS attack, and Heartleech
IoTPOT dataset	Normal, Malware
MQTT-IoT	Aggressive scan (Scan A) User Datagram Protocol (UDP) scan (Scan sU) Sparta SSH brute-force (Sparta) MQTT brute-force attack (MQTT BF)
IoTID20 dataset	Normal DoS, Mirai, MITM, Scan

4.1 DARPA dataset

According to the network traffic and audit logs, the DARPA dataset was first made public in February 1998 [27]. The training data encompasses seven weeks of network-based attacks, whereas the testing data consists of two weeks of network-based attacks. However, the disadvantage of this dataset it does not display real-world network traffic [28].

4.2 KDD Cup 1999 dataset

The KDDCUP99 dataset was illustrated in [29] based on the DARPA'98 IDS evaluation program [30]. Moreover, many researchers have widely used this dataset for evaluating anomaly detection approaches. There are 4 GB of tcpdump data which is collected in seven weeks of network traffic in the DARPA'98 dataset. The dataset is labeled as attack or normal data. Additionally, there are approximately 4,900,000 single vector connections in which each consists of 41 features in the training data of the dataset. There are four types of attacks, such as Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probe attacks, in this dataset [31].

4.3 NSL-KDD dataset

The NSL-KDD dataset was expanded from the KDDCUP99 dataset, in which selected records were extracted from the entire KDDCUP99 dataset. In study [31], the researchers have confirmed that the KDDCUP99 dataset greatly affects the performance of the evaluated systems and leads to poor evaluation of anomaly detection techniques. Therefore, these researchers proposed the NSL-KDD, which excludes redundant records in the train set, and the proposed test sets do not contain duplicate records. On the other hand, for each difficulty level the number of records chosen are inversely proportional to the percentage of records in the KDDCUP99 dataset, the train and test sets records are reasonable. The NSL-KDD dataset includes four attack types, such as DoS, U2R, R2L, and Probe attacks.

4.4 UNSW-NB15 dataset

The UNSW-NB15 dataset which is a labelled dataset was developed in 2015. There are a combination of contemporary synthesized attack data and real modern normal in this dataset and consists of a total of 47 features. Moreover, this dataset encompasses nine types of attacks, known as fuzzes, analysis, backdoors, DoS, exploits, generic, reconnaissance shellcode, and worm attack types [32].

4.5 KYOTO dataset

The Kyoto dataset was developed in 2006 for IDS research. This dataset is built based on 3 years of real network traffic data. The dataset consists of 14 features derived from

the KDDCUP99 and 10 extra features. Further, their honeypot data totally consists of 43,043,255 attack sessions and 50,033,015 normal sessions. In addition, three attack types, such as exploits, shellcodes, and malware are discussed in this dataset [33].

4.6 CICDS2017 dataset

The CICIDS2017 dataset was established through the Canadian Institute for Cybersecurity (CIC) in 2017. This dataset includes attack network traffic data and real world benign. There are 80 features based on 225,746 records in the CICIDS2017 dataset. Additionally, there are five types of attacks, such as Brute Force, Web, DoS, Botnet, and DDoS in this dataset [34].

4.7 CIDDS- 001

The CIDDS- 001 which is a labelled flow-based dataset was created for the anomaly-based NIDS evaluation. There are normal and attack traffic data which are obtained over the period of four weeks in this dataset. Additionally, this dataset contains 14 features and four attack types, such as DoS, PortScan, Brute Force, and Ping Scan [35].

4.8 CSE-CIC-IDS2018

The CSE-CIC-IDS2018 was developed by the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC) [36]. This dataset consists of seven different types of attacks, such as Heartbleed, Brute-force, DoS, DDoS, Web attacks, Botnet, and infiltration. It is similar to the CICDS2017 dataset [37], the CICFlowMeter tool [38] is ultilized to obtain 80 network flow features from the generated network traffic.

4.9 IoTPOT

The IoTPOT was established through honeypots, so there was no process for manual labeling and anonymization. However, it has restricted view of the network traffic since only attacks launched at the honeypots could be observed. Authors claim that IoTPoT examines Telnet-based attacks against different IoT devices running on different CPU architectures such as MIPS, ARM and PPC. During 39 days of operation, authors recorded 76,605 download attempts of malware binaries from 16,934 visiting IP. Authors further claim that none of these binaries could have been detected by existing honeypots that handle the Telnet protocol, such as telnet password honeypot and honeyd, because these honeypots are not capable of handling different incoming commands initiated by the attackers [39].

4.10 MQTT-IoT

The Message Queuing Telemetry Transport (MQTT) dataset is an IoT dataset concentrated on MQTT communications. This dataset was developed through using IoT-Flock [40], a network traffic generator tool able to emulate IoT devices and networks based on MQTT and CoAP protocols. IoT-Flock provides the ability to configure the network scenario, in terms of nodes (e.g., sensor type, IP addresses, listening ports, etc.) and communications (e.g., time interval used for communications between the sensors and the broker). In addition, the tool implements different cyber-threats against the MQTT and CoAP: publish flood, packet crafting attacks, segmentation fault attack against CoAP (making use of a null Uri-path), and memory leak attacks against CoAP (by using invalid CoAP options during packets forging) [41].

4.11 IoTID20 dataset

The IoTID20 dataset was generated based on [42]. The new IoT botnet dataset has a more comprehensive network and flow-based features. The flow-based feature can be used to analyze and evaluate a flow-based intrusion detection system. The proposed IoT botnet dataset provides a reference point to identify anomalous activity across the IoT networks. The IoT Botnet dataset can be accessed from [43]. The new IoTID20 dataset will provide a foundation for the development of new intrusion detection techniques in IoT networks [44].

5. Review evaluation measures

In this study, we implemented a survey as shown in *Table 4* to observe the different evaluation measurements to evaluate the performance of the IDS. We also list the popular and effective evaluation measurements which is indicated in *Fig. 1*. The subsections below reveal detailed contents of these measures.

Table 4 Measurement metrics in current studies

Studies	Measurements Metrics
[45]	Precision, Recall, F-1 score and False Alarm Rate (FAR)
[16]	Misclassification rate, recall, FP rate, Specificity, Precision
[46]	Detection rate, Classification accuracy
[15]	Confusion matrix, F-measure
[47]	Confusion matrix, Accuracy, Precision, Sensitivity, Specificity F1, Detection rate, False alarm rate
[48]	Confusion matrix, Detection rate, Accuracy, Precision, False-positive Rate, Mathew correlation coefficient (MCC), Cohen's Kappa K
[49]	Overall accuracy, Detection rate, False alarm rate, TPR, FPR
[26]	Accuracy, error rate, Precision, Recall, Specificity, F-score, MCC
[50]	Accuracy, Precision, Receiver operating characteristic (ROC) curve

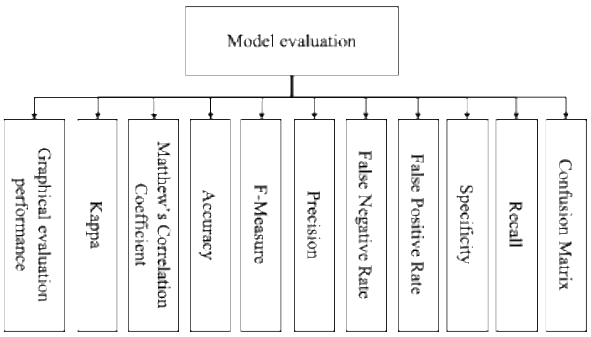

Fig. 1 Model evaluation metrics

5.1 Confusion Matrix

The confusion matrix as indicated in *Table 5* is the sum of the results predicted by the classification model. The confusion matrix is derived by summing the total number of correct and false classified predictions based on each class [51]. It is necessary to derive the following values before designing the confusion matrix [52]:

(a) **True Positive (TP)**: The true positive values refer to the number of instances that has been correctly classified by the model.
(b) **True Negative (TN)**: The true negative values are the number of negative instances that were correctly classified by the model.
(c) **False Positive (FP)**: False positive value is the number of negative instances labelled incorrectly as positive instances.
(d) **False Negative (FN)**: False negative value is the number of positive instances labelled incorrectly as negative instances.

Table 5 Confusion matrix

		Predicted Values	
	Class	Negative (0)	Positive (1)
Actual Values	Negative (0)	True Negative (TN)	False Positive (FP)
	Positive (1)	False Negative (FN)	True Positive (TP)

5.2 Recall

Recall also referred to as sensitivity or true positive rate refers to the proportion of real positive instances that have been predicted positive[53]. Recall can be calculated using the below formula.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (1)$$

5.3 Specificity

Specificity describes the effectiveness of the classification model in identifying negative labels [54]. Specificity is calculated using the below formula.

$$Specificity = \frac{TN}{TN + FP} \quad (2)$$

5.4 False Positive Rate (FPR)/ False Alarm Rate (FAR)

The FPR also called the Fall-Out is the proportion on negative instances classified incorrectly as positive instances. In simpler terms, probability of false alarms to be raised [55]. The FPR is calculated using the below formula.

$$False\ Positive\ Rate = \frac{FP}{TN + FP} \quad (3)$$

5.5 False Negative Rate (FNR)/ Undetected Rate (UR)

The FNR refers to the proportion of incorrectly classified samples to the number of positive samples [56]. The FNR is calculated using the below formula.

$$FNR = \frac{FN}{TP + FN} \quad (4)$$

5.6 Precision

The precision is the proportion of predicted positives that are real positives. Precision is applied on a variety of areas such as, machine learning, data mining, and information retrieval [57]. Precision is calculated using the below formula:

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

5.7 F-Measure

The f-measure is considered as the harmonic mean of the precision and recall [58]. The f-measure is calculated using the below mathematical equation.

$$F1 = \frac{Precision * Recall}{Precision + Recall} \quad (6)$$

5.8 Accuracy

The accuracy is expressed as the overall effectiveness of the classification model [54]. The formula used for the calculation of the accuracy is as follows:

$$ACC = \frac{TP + TN}{TP + FP + TN + FN} \quad (7)$$

5.9 Matthew's Correlation Coefficient (MCC)

The MCC is an approach utilized to measure the quality of binary and multiclass classification. The MCC values is ranged from +1 to −1, where +1 shows total agreement , 0 illustres random predications and −1 indicates total disagreement [59]. The MCC can be calculated using the below formula:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \quad (8)$$

5.10 Kappa

Kappa also referred to as Cohen's Kappa is a measure of the inter-reliability. Kappa is recognized to be more robust rather than the straightforward percent agreement approach. The values of Kappa are ranged from 0–1. *Table 6* shows the ranges of value and contribution of the model based on these values [60].

Table 6 Kappa measurement

Values	Model contribution
0–0.20	No Agreement
0.21–0.39	Slight Agreement
0.40–0.59	Fair Agreement
0.60–0.79	Substantial Agreement
0.80–0.90	Almost Perfect

The calculation of Kappa is expressed below formula:

$$k = \frac{P_o - P_e}{1 - P_e} = 1 - \frac{1 - P_o}{1 - P_e} \quad (9)$$

5.11 Graphical evaluation performance

The Receiver Characteristic Operator (ROC) curve which is a graphical evaluation describes the diagnostic capability of a binary classifier system since its taxonomy threshold is different. The ROC curve is established by plotting the ratio of true positive versus false positive rates. The Area Under the Curve (AUC) measures the whole two-dimensional area under the whole ROC curve [61]. The AUC can assess models by overall performance, so it is more considered in model evaluation. The suggestion of the following scale for AUC value interpretation is shown in Table 7 [62].

Table 7 AUC Performance

AUC value	**Performance of Model**
0.9 – 1.0	Excellent
0.8 – 0.9	Very good
0.7 – 0.8	Good
0.6 – 0.7	Fair
0.5 – 0.6	Poor

6. Open challenges and future directions

In this section, we want to discuss the challenges and future directions. The first major challenge is the lack of available datasets. The datasets play an important role in establishing IDSs. In order to achieve

robustness IDSs, it is necessary to update modern attacks, but the existing datasets are too old to reflect these new attacks. Developing new datasets depends on expert knowledge, time-consumption, and high cost. Moreover, the change of the Internet environment increases the lack of data. Ideally, the datasets consist of most popular attacks and correspond to current network environments. In addition, the available datasets are representative, balanced and have less redundancy and less noise. The solution for this problem is systematic datasets construction and incremental learning.

The second one is low detection accuracy performances in actual environments. As discussed in section 3, in some cases, ML/DL methods do not perform well in detecting IDSs in actual environments. This is simply because most of current studies were implemented employing labeled datasets while but the datasets in the practice are more complex. Therefore, when the dataset does not include all real-world typical samples, the performance in the real world is not good even if the models obtain high accuracy on test sets.

Furthermore, based on the survey of the recent studies, we conclude the major trends of IDSs research as follows. First, combining domain knowledge with ML/DL can improve the detection effect, especially when the goal is to recognize specific types of attacks in specific application scenarios. Second, improvements in ML/DL algorithms are the main goals to enhance the detection effect. Thus, studies involving deep learning and unsupervised learning methods have an increasing trend. Last but not least, we need to develop practical models. Because the practical IDSs not only need to have high detection accuracy but also high runtime efficiency and interpretability.

7. Conclusions

The use of IoT devices has increased significantly in our lives owing to the ability to convert objects from different application domains into Internet servers. The privacy and security of users are threatened because of IoT security vulnerabilities. Consequently, it is crucial to construct more robust security solutions for IoT. ML/DL-based IDSs is one of the pivotal techniques for IoT security. In this study, a survey of ML/DL based intrusion detection techniques used in IDSs for IoT networks and systems is illustrated. The different IDS types, popular ML/DL approaches, datasets, and evaluation classification measurements have been discussed in detail. We also recognize the advantages and limitations of each ML/DL method in detecting attacks. The open challenges and future direction are summarized. This work attempts to provide the summarized but comprehensive and useful insight into the various security challenges currently being faced by IoT systems and networks and possible solutions, with a focus on intrusion detection, based on ML/DL based methods.

References

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[2] I. Lee and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, 2015, doi: 10.1016/j.bushor.2015.03.008.

[3] Joseph Bradley, J. Barbier, and D. Handler, “Embracing the Internet of Everything To Capture Your Share of $ 14 . 4 Trillion,” *Cisco Ibsg Gr.*, p. 2013, 2013, [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of things: The road ahead,” *Comput. Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

[5] D. Singh, G. Tripathi, and A. J. Jara, “A survey of Internet-of-Things: Future vision, architecture, challenges and services,” *2014 IEEE World Forum*

Internet Things, WF-IoT 2014, pp. 287–292, 2014, doi: 10.1109/WF-IoT.2014.6803174.

[6] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.

[7] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017, [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2017.02.009.

[8] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.

[9] H. Ouechtati and N. Ben Azzouna, "Trust-ABAC towards an access control system for the internet of things," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10232 LNCS, pp. 75–89, 2017, doi: 10.1007/978-3-319-57186-7_7.

[10] R. Damasevicius *et al.*, "An annotated real-world network flow dataset for network intrusion detection," *Electron.*, vol. 9, no. 5, 2020, doi: 10.3390/electronics9050800.

[11] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[12] N. A. Azeez, T. J. Ayemobola, S. Misra, R. Maskeliūnas, and R. Damaševičius, "Network intrusion detection with a hashing based apriori algorithm using Hadoop MapReduce," *Computers*, vol. 8, no. 4, 2019, doi: 10.3390/computers8040086.

[13] T. A. Mohamed, T. Otsuka, and T. Ito, *Towards machine learning based IoT intrusion detection service*, vol. 10868 LNAI. Springer International Publishing, 2018.

[14] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study," 2020, [Online]. Available: http://arxiv.org/abs/2006.15340.

[15] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, 2019, doi: 10.1109/JIOT.2019.2926365.

[16] A. Alghuried, "A Model for Anomalies Detection in Internet of Things (IoT) Using Inverse Weight Clustering and Decision Tree," p. 64, 2017, doi: 10.21427/D7WK7S.

[17] A. Verma and V. Ranga, "Machine Learning Based Intrusion Detection Systems for IoT Applications," *Wirel. Pers. Commun.*, vol. 111, no. 4, pp. 2287–2310, 2020, doi: 10.1007/s11277-019-06986-8.

[18] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019, doi: 10.1109/ACCESS.2019.2903723.

[19] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," *arXiv*, 2019.

[20] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," *Sensors (Switzerland)*, vol. 19, no. 9, 2019, doi: 10.3390/s19091977.

[21] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *J. Inf. Secur. Appl.*, vol. 41, pp. 1–11, 2018, doi: 10.1016/j.jisa.2018.05.002.

[22] Y. Li *et al.*, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Meas. J. Int. Meas. Confed.*, vol. 154, p. 107450, 2020, doi: 10.1016/j.measurement.2019.107450.

[23] E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," *2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016*, pp. 4–9, 2016, doi:

10.1109/ISNCC.2016.7746067.

[24] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, 2018, doi: 10.1109/IJCNN.2018.8489489.

[25] R. Xu, Y. Cheng, Z. Liu, Y. Xie, and Y. Yang, "Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services," *Futur. Gener. Comput. Syst.*, vol. 112, pp. 228–242, 2020, doi: 10.1016/j.future.2020.05.035.

[26] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. dos S. Vieira, "Hybrid approach to intrusion detection in fog-based IoT environments," *Comput. Networks*, vol. 180, 2020, doi: 10.1016/j.comnet.2020.107417.

[27] "1998 DARPA intrusion detection evaluation dataset." https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset (accessed Mar. 17, 2021).

[28] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "A detailed analysis of the CICIDS2017 data set," *Commun. Comput. Inf. Sci.*, vol. 977, no. Cic, pp. 172–188, 2019, [Online]. Available: http://dx.doi.org/10.1007/978-3-030-25109-3_9.

[29] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Cost-based modeling for fraud and intrusion detection: Results from the JAM project," *Proc. - DARPA Inf. Surviv. Conf. Expo. DISCEX 2000*, vol. 2, pp. 130–144, 2000.

[30] R. P. Lippmann *et al.*, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," *Proc. - DARPA Inf. Surviv. Conf. Expo. DISCEX 2000*, vol. 2, pp. 12–26, 2000.

[31] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symp. Comput. Intell. Secur. Def. Appl. CISDA 2009*, no. Cisda, pp. 1–6, 2009.

[32] S. A. V. Jatti and V. J. K. Kishor Sontif, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 3976–3983, 2019.

[33] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," *Proc. 1st Work. Build. Anal. Datasets Gather. Exp. Returns Secur. BADGERS 2011*, pp. 29–36, 2011.

[34] D. Aksu, S. Üstebay, M. A. Aydin, and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning Techniques and fisher score feature selection algorithm," 2018.

[35] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for network intrusion detection systems using sistance-based machine learning," *Procedia Comput. Sci.*, vol. 125, pp. 709–716, 2018.

[36] "CSE-CIC-IDS2018." https://www.unb.ca/cic/datasets/ids-2018.html (accessed Mar. 17, 2021).

[37] "Intrusion detection evaluation dataset." https://www.unb.ca/cic/datasets/ids-2017.html (accessed Mar. 17, 2021).

[38] "CICFlowMeter." https://www.unb.ca/cic/research/applications.html#CICFlowMeter (accessed Mar. 17, 2021).

[39] Y. M. Pa Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: Analysing the rise of IoT compromises," *9th USENIX Work. Offensive Technol. WOOT 2015*, 2015.

[40] S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT-flock: an open-source framework for IoT traffic generation," *2020 Int. Conf. Emerg. Trends Smart Technol. ICETST 2020*, 2020.

[41] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, "MQTTset, a new dataset for machine learning techniques on MQTT," *Sensors (Switzerland)*, vol. 20, no. 22, pp. 1–17, 2020.

[42] H. Kang, D. H. Ahn, G. M. Lee, J. Do Yoo, K. H. Park, and H. K. Kim, "IoT network intrusion datase." https://ieee-dataport.org/open-access/iot-network-intrusion-dataset (accessed Mar. 17, 2021).

[43] "IoT intrusion dataset 2020." https://sites.google.com/view/iot-network-intrusion-dataset (accessed Mar. 17,

2021).

[44] I. Ullah and Q. H. Mahmoud, "A scheme for generating a dataset for anomalous activity detection in IoT networks," *Adv. Artif. Intell. Can. AI 2020. Lect. Notes Comput. Sci.*, vol. 12109, 2020, doi: 10.1007/978-3-030-47358-7_37.

[45] B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," *2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018*, pp. 1–6, 2019, doi: 10.1109/ATNAC.2018.8615294.

[46] P. Li and Y. Zhang, "A Novel Intrusion Detection Method for Internet of Things," *Proc. 31st Chinese Control Decis. Conf. CCDC 2019*, pp. 4761–4765, 2019, doi: 10.1109/CCDC.2019.8832753.

[47] K. V. V. N. L. Sai Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, "Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 2372–2379, 2020, doi: 10.1016/j.procs.2020.04.257.

[48] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul. Model. Pract. Theory*, vol. 101, no. November 2019, p. 102031, 2020, doi: 10.1016/j.simpat.2019.102031.

[49] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things," *J. Commun. Networks*, vol. 20, no. 3, pp. 291–298, 2018, doi: 10.1109/JCN.2018.000041.

[50] B. Susilo and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm," *Inf.*, vol. 11, no. 5, 2020, doi: 10.3390/INFO11050279.

[51] R. K. Fleischman and L. D. Parker, "Introduction 1," *What is Past is Prologue*, pp. 3–19, 2018, doi: 10.4324/9781315165851-1.

[52] "What is a Confusion Matrix in Machine Learning." .

[53] J. Han, M. Kamber, and J. Pei, *Data Mining Concepts and Techniques*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2011.

[54] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Inf. Process. Manag.*, vol. 45, no. 4, pp. 427–437, 2009, doi: 10.1016/j.ipm.2009.03.002.

[55] "What is a False Positive Rate?" https://www.pico.net/kb/what-is-a-false-positive-rate (accessed Dec. 18, 2020).

[56] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[57] D. M. W. Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation," pp. 37–63, 2020, [Online]. Available: http://arxiv.org/abs/2010.16061.

[58] D.-L. LIU, X. LIU, H. YU, W.-T. WANG, X.-H. ZHAO, and J.-F. CHEN, "A Multilevel Deep Learning Method for Data Fusion and Anomaly Detection of Power Big Data," vol. 131, no. Eeeis, pp. 533–539, 2017, doi: 10.2991/eeeis-17.2017.79.

[59] B. W. Matthews, "Comparison of the predicted and observed secondary structure of T4 phage lysozyme," *BBA - Protein Struct.*, vol. 405, no. 2, pp. 442–451, 1975, doi: 10.1016/0005-2795(75)90109-9.

[60] M. L. McHugh, "Lessons in biostatistics interrater reliability : the kappa statistic," *Biochem. Medica*, vol. 22, no. 3, pp. 276–282, 2012, [Online]. Available: https://hrcak.srce.hr/89395.

[61] "Towards data science." https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5 (accessed Feb. 22, 2021).

[62] M. Bekkar, H. K. Djemaa, and T. A. Alitouche, "Evaluation measures for models assessment over imbalanced data sets," *J. Inf. Eng. Appl.*, vol. 3, no. 10, pp. 27–38, 2013, [Online]. Available: http://www.iiste.org/Journals/index.php/JIEA/article/view/7633.