

# A review on machine learning based intrusion detection system for internet of things enabled environment

Nisha, Nasib Singh Gill, Preeti Gulia

Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, India

## Article Info

### Article history:

Received Jul 2, 2023

Revised Oct 12, 2023

Accepted Nov 29, 2023

### Keywords:

Attacks in internet of things  
Environment  
Internet of things  
Internet of things security  
Intrusion detection system  
Machine learning

## ABSTRACT

Within an internet of things (IoT) environment, the fundamental purpose of various devices is to gather the abundant amount of data that is being generated and then transmit this data to the predetermined server over the internet. IoT connects billions of objects and the internet to communicate without human intervention. But network security and privacy issues are increasing very fast, in today's world. Because of the prevalence of technological advancement in regular activities, internet security has evolved into a necessary requirement. Because technology is integrated into every aspect of contemporary life, cyberattacks on the internet of things represent a bigger danger than attacks against traditional networks. Researchers have found that combining machine learning techniques into an intrusion detection system (IDS) is an efficient way to get beyond the limitations of conventional IDSs in an IoT context. This research presents a comprehensive literature assessment and develops an intrusion detection system that makes use of machine learning techniques to address security problems in an IoT environment. Along with a comprehensive look at the state of the art in terms of intrusion detection systems for IoT-enabled environments, this study also examines the attributes of approaches, common datasets, and existing methods utilized to construct such systems.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Nisha

Department of Computer Science and Applications, Maharshi Dayanand University

Rohtak, Haryana, India

Email: nisha.rs.dcsa@mdurohtak.ac.in

## 1. INTRODUCTION

With the advent of the internet of things (IoT), computers have been imagined as everyday objects that can sense their environment, form relationships with one another, and share information with one another and the rest of the world over the Internet. The fundamental goal of IoT is to increase productivity and speed up the delivery of critical information by having self-reported machines in a real-time setting. There have been significant advancements in user experience in recent years thanks to IoT-based frameworks in fields as diverse as smart farming, intelligent healthcare system, supply chain management, smart housing, and intelligent transportation system [1], [2]. IoT devices are typically embedded with sensors, which monitor and control the information over the internet for making the best decisions. By 2025, there will be 41.6 billion IoT devices, and they will produce 79.4 zettabytes of data [3], according to the international data corporation (IDC). This technological advancement provides enormous benefits to consumers, but the IoT has recently faced significant challenges due to security issues caused by equipment failure and malicious attacks led by external intruders. IoT networks are extremely susceptible to online threats like distributed denial-of-service (DDoS) assaults [4]. The variety of devices as well as protocols, direct accessibility of equipment to the Internet, as well as resource limits on devices, are all factors that make it difficult to protect

internet of things devices from being attacker [5]. An intrusion occurs whenever there is an attempt to compromise the security, privacy, or availability of a system's resources [6]. Therefore, a specialized component is necessary for protecting IoT networks. Increasing the intrusion detection system (IDS) capabilities of wireless networks can help protect the IoT network against attacks and other vulnerabilities [7]. As a result, IDSs are required to detect attacks so that IoT networks can continue to be reliable and accessible. As the primary function of IDS is to detect attacks, it is crucial to define the many threats that can arise in an IoT environment. Sybil attacks, selective forwarding attacks, service assaults, wormhole attacks, sinkhole attacks, fake data attacks, black hole attacks, jammer attacks, and so on are all examples of key attacks in the internet of things. Figure 1 depicts many sorts of attacks in the IoT context.

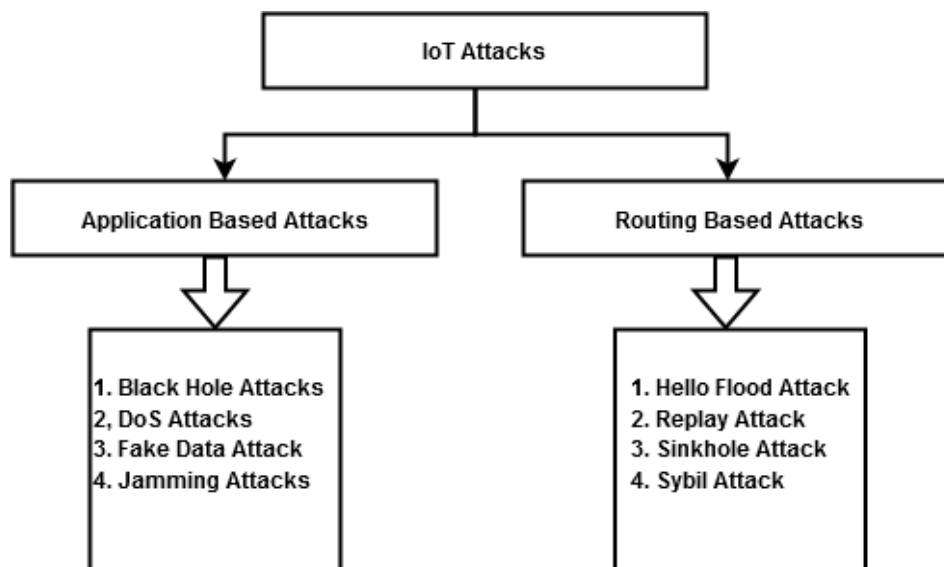


Figure 1. Attacks in IoT environment

Wormhole attack (routing-based assault), as explained by Deshmukh-Bhosale and Sonavane [8] in their study work, involves simultaneous attacks or penetrations from two different directions in order to reach the intended node. This study effort is praised for detecting nearby networks and calculating the effects of threats. Rathore and Park [9] focused on the effects of the Sybil attack, where the node generates many identities, resulting in a variety of routing protocols. To detect such assaults, detection techniques and spoofing mechanisms are needed. Lyu *et al.* [10] presented intrusion detection methodology to identify hostile users on IoT networks. In particular, the focus was on denial-of-service attacks, in which the attacker attempts to take control of a node by overwhelming its resources. Furthermore, because the Internet of Things devices frequently perform in an unsupervised environment, an adversary with malicious intent can get physical access to these devices [11]. As a result, cyber-attacks are more likely to affect Internet of Things platforms than traditional computer networks.

## 2. MACHINE LEARNING APPROACHES FOR IDS

Machine learning's ultimate goal is to endow machines with the capacity for autonomous learning and decision-making, on par with human beings. Algorithms trained with machine learning utilize statistical methods to examine large data sets for recurring patterns, then use that information to inform future decisions and forecasts [12], [13]. Here, we give a brief introduction to the various machine-learning strategies currently being used by IDSs in the IoT landscape (IDSs). In Table 1, a concise review of machine learning (ML) approaches, including their benefits and drawbacks, as well as references to relevant research work that has been carried out, is provided. The most prevalent machine learning approaches that are utilized for creating IDSs in IoT systems are shown in Figure 2.

It is possible to utilize a variety of techniques to protect the backend IoT networks. Supervised learning is more successful when the environment variable is known (the outcome should be the same for every input). In cases where the outcome is irrelevant, unsupervised learning is employed; this type of learning is typically used to classify the attributes.

Figure 3 depicts the supervised learning algorithm, random forest. There is a one-to-one correlation between the density of a forest and the reliability of the decisions made using different types of decision trees. The algorithm's fundamental component is a decision tree, which also acts as a decision aid. Using a tree-like graph, we may depict several outcomes. These methods can be used for both classification and regression. In supervised learning, the support vector machine is a popular technique (SVM). It works well with both categorization and statistical analysis. However, it is mainly applied to categorization issues. See Figure 4 for an illustration of how this classification method works to locate the hyperplane that demarcates the two groups. The value of a specific coordinator is used here to represent each data point.

Table 1. A taxonomy of ML-based security techniques for internet of things systems

ML method	Attack types handled	Pros	Cons	Results
KB [14]	HTTP attacks (buffer overflow, shell attacks), DoS, probe, R2L	The training just needs a relatively small number of samples. It is able to categorize using both binary as well as multi-systems simultaneously.	It does not take into consideration the interdependencies between characteristics for the sake of categorization; hence, its accuracy suffers as a result.	Accuracy=87.7% Precision=97.7% and F-measure=87.7%
KNN [15]	U2R, R2L, Flooding attacks, DoS, DDoS	Easy to be using.	The most difficult parts of this process are finding missing nodes as well as determining the ideal value of K.	Recall=89.7% Precision=90.7% and F-measure=90.7%
DT [16]	DDoS, U2R, R2L	This method is less complicated and easy to use.	The storage space must increase. It is difficult to process computationally	Recall=95.7% Accuracy=95.7% and F-measure=95.7%
SVM [17]	Scan, DDoS (TCP, UDP flood), port sweep	SVMs may perform tasks such as online learning and real-time anomaly-based intruder detection. This is made possible by their simplicity, which makes them very scalable. SVMs make far less use of storage as well as memory.	When we cannot split information linearly, SVM is used to classify it, but it remains difficult to reach the needed classification speed by employing a perfect kernel function.	Accuracy=88.7% Precision=88.7% and F-measure=88.7%
EL [18]	DoS, Probe, R2L, U2R attacks	It can withstand excessive or improper fitment. Operates at a higher level of efficiency than a single classification. It helps to reduce the amount of variation.	The usage of numerous classifiers in parallel leads to an increase in the temporal complexity of the process.	Recall=93.7% Precision=93.7% and F-measure=93.7%
RF [19]	DoS, Probe, R2L, U2R	It generates an output that is more reliable and accurate, as well as one that is sensitive to overfitting. It takes a far lower number of inputs than other methods, and it does away with the need for feature selection altogether.	Real-time programs that need a huge dataset may not find it feasible to employ RF since it creates several DTs, hence this may make its usage difficult.	Recall=92.7% Precision=92.7% and F-measure=92.7%

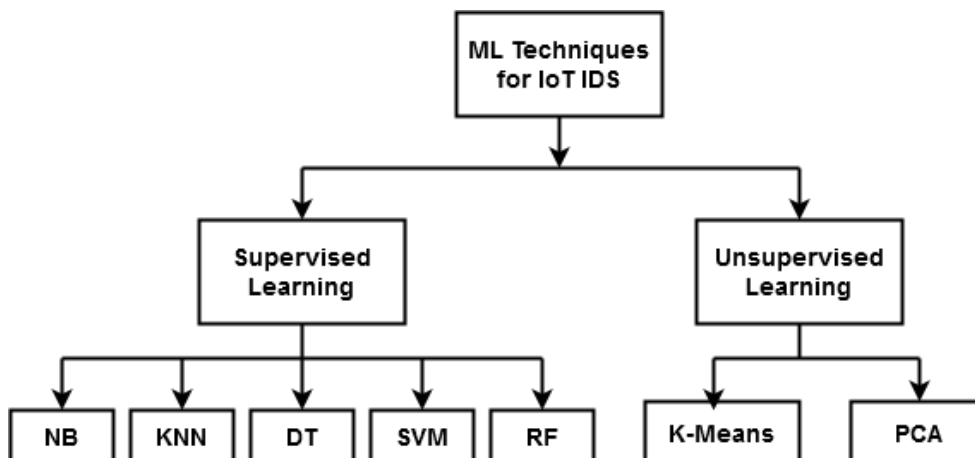


Figure 2. Intrusion detection solutions for the internet of things that make use of machine learning

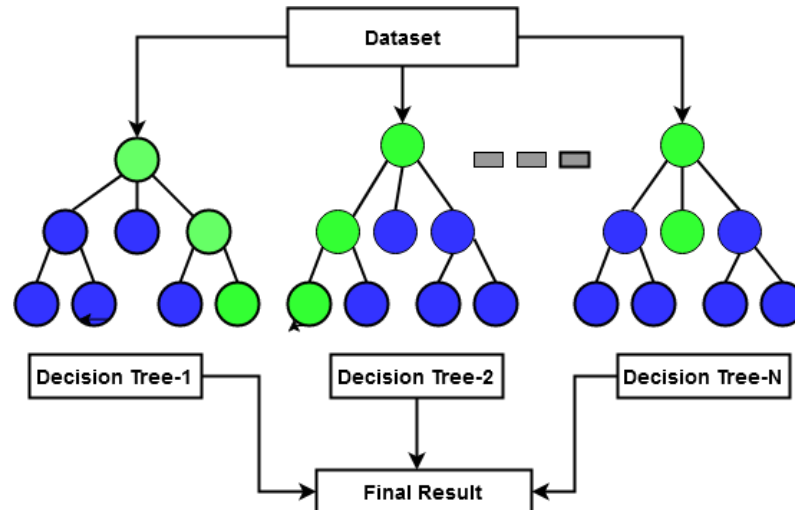


Figure 3. Random forest in machine learning

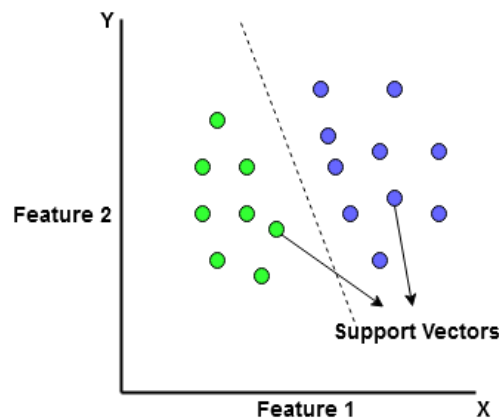


Figure 4. SVM in machine learning

### 3. APPLICATIONS OF MACHINE LEARNING IN THE INTERNET OF THINGS FOR IDS

A multi-layered deeper RNN model was presented by Almiani *et al.* [20] to be used for Internet of Things devices. DoS, Probe, U2R, as well as R2L attack detection rates, were determined to be 98.26%, 97.36%, 64.94%, and 77.24% correspondingly after the performance was assessed using the NSL-KDD database. This study presents a nearly flawless detection approach for defending against cyberattacks, as shown by the experimental as well as performance analyses. An IDS integrated data sampling method to solve the class imbalance is presented by Qaddoura *et al.* [21], this IDS proposal consists of three steps, namely integrated cluster, classification, as well as oversampling methods. The issue of there being no minority class is addressed via the use of oversampling. The work of Saravanan *et al.* [22] examines both traditional ML methods and NIDS, as well as potential future directions. Since learning methods provide covert security and performance in the background, we focus on IoT NIDS for Machine Learning in this study. It offers a comprehensive look into NIDSs that use many features of internet-based learning approaches, complementing other prominent surveys that deal with common frames. It also protects individuals from typical IoT NIDS because of the survey's emphasis on prevention. Various kind of attacks like phishing, probe, and eavesdropping, may take place in IoT ecosystem as shown in Figure 5.

A new concept presented by Papafotikas *et al.* [23], successfully detects the suspicious behavior of smart items in an internet of things (IoT) environment, which was caused by a virus assault on an IoT node. To spot suspicious behavior and benefit from the dissipation of current supply characteristics, machine learning (ML) based clustering method is founded on the K-means clustering algorithm and supervised training. The goal of this study is to develop an external current monitoring device for obtaining intrusion detection based on the operating parameters of the equipment under monitoring. Latif *et al.* [24] presented a

novel technique for detecting attacks in the industrial IoT utilizing the random neural network (RNN), a recent and lightweight ANN algorithm. Gradient descent is used to train the recommended RNN model (GD). During dataset processing, the “Source ID” characteristic is removed to improve accuracy to greater than 99%. Saranya *et al.* [25] examine the IoT, big data, smart cities, fog computing, and 5G networks as application cases in their study of ML algorithms for intrusion detection systems (GN). To further classify the intrusions, we employ ML approaches such as linear discriminant analysis, classification and regression trees, and random forest. As this study shows, the detection rate, false positive rate, and accuracy all change based on the algorithm and the application. Using a number of different types of machine learning, Shaver *et al.* [26] developed an anomaly-based intrusion detection system to safeguard IoT devices. Since the attack's signature will not be recognized, but the resulting network activity will deviate from typical patterns, the IDS will be able to detect a zero-day attack and take corrective action. This research examines the novel IoT network intrusion dataset. Tawalbeh *et al.* [27] proposed an innovative generic and expanded IoT model with cloud/edge assistance to identify security and privacy components at each IoT layer. Amazon web science virtual machine (AWS) was created as the IoT model's lower layer. The Raspberry Pi4 hardware package was presented at the IoT framework's middle layer. The top layer is deployed using AWS cloud-enabled IoT. In the described IoT cloud/edge concept, data transfer between the layers was made possible with the use of security credentials. To solve the issues of Signature-based intrusion detection systems (SIDS) and anomaly-based intrusion detection systems (AIDS), Khraisat *et al.* [28] developed a hybrid intrusion detection system (HIDS) (anomaly-based intrusion detection). Combining a C5 classifier and a one-class support vector classifier, HIDS provides an additional layer of protection for IoT devices. Using the BoT-IoT dataset, the proposed HIDS is tested against a wide range of threats, including DDoS assaults, OS and service scanning, key loggers, and data exfiltration. The problem of duplicated features has been addressed by Albulayhi *et al.* [29] devised and implemented a novel approach called minimal redundancies discriminative feature selection (MRD-FS). The distinguishing characteristics have been chosen by applying two standards, namely, representativeness and redundancy, to the selection process. The BoT-IoT dataset served as the basis for their model's evaluation.

$$IG = HY - HYX = HX - H(X|Y) \quad (1)$$

The expression gives the definition of  $y$ 's entropy.

$$Hy = - \sum y \log_2(p(y)) \quad (2)$$

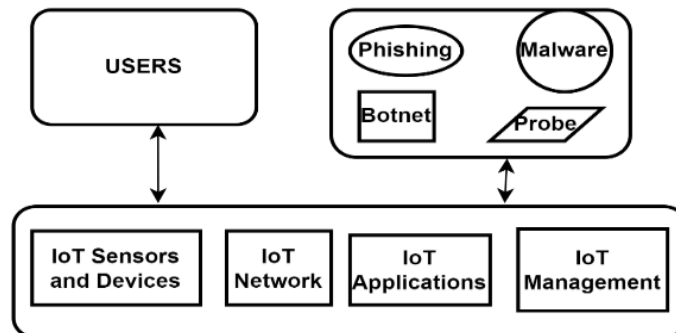


Figure 5. A representation of the connections between the IoT ecosystem and possible dangers

Garg *et al.* [30] used techniques such as grey wolf optimizing (GWO) as well as convolutional neural network (CNN) in the hybrid data process theory for the purpose of detecting network anomalies. According to the authors, their model was able to obtain a higher accuracy as well as detection rate in contrast to previous IDSs considered as the state-of-the-art. Saheed *et al.* [31] created an intrusion detection system for detecting threats in IoT networks using machine learning techniques. To detect attacks in less secure IoT networks, researchers primarily used supervised machine learning algorithms and the UNSWNB-15 dataset. With 99.99% accuracy, the proposed model reduced communication overhead. In the future, this model can be improved using deep learning methods on BoT-IoT datasets and can compare results to UNSWNB-15 datasets. Table 2 shows the results and limitations of classification techniques available for IoT threats.

Table 2. Results and limitations of classification techniques available for internet of things threats

Research Paper	Year	Methodology	Results	Limitations
[32]	2016	The K-means clustering method using empirical likelihood and support vector machines	Achieving an accuracy of 96.02%, a TP rate of 76.19%, and an F rate of 5.92%	Having a high rate of false positives and low true positives
[33]	2016	Connectivity systems modeled after ant colonies that operate autonomously	Both the DoS and Probe attacks are highly accurate, at 99.79% and 98.55%, respectively.	The dataset used in this research is not representative of current-day attacks.
[34]	2017	Models using DNNs and shallow NNs	In terms of accuracy, shallow NN achieves 96.75%, whereas deep NN achieves 98.27%.	As unfortunate as it is, the NSLKDD dataset that was employed does not adequately capture the features of modern assaults.
[35]	2018	NB	With an F-measure of 97.7 and an accuracy of 99.3 on average, recall is extremely high.	The created dataset's features do not reflect real-world network behavior.
[36]	2018	ELM	83% accuracy	training time is High
[37]	2019	As a means of dimensionality reduction, we employ LDA with NB and CF.	The false alarm rate is 5.56 percent and the accuracy= is 84.82	High false-positive rate and low sensitivity
[38]	2020	Decision tree	The F1 score is 99.98, the accuracy score is 99.98, the precision score is 97.38, and the recall score is 97.39.	A long period is required for model training

#### 4. COMPARISON OF PUBLICALLY AVAILABLE IDS DATASETS

Given the prevalence of machine learning approaches in the fight against AIDS, it is crucial to evaluate these methods using appropriate datasets. The tabulated properties of the datasets are shown in Table 3. According to our findings, traditional data sets like KDD'99, which were designed for wired networks, would not help you build effective IDS for the IoT.

Saba *et al.* [39] proposed a two-stage hybrid model for detecting traffic offenses. At this stage, the genetic algorithm is used to enhance the quality of the proposed model. The second step involves evaluating the model with a battery of machine learning tools, such as support vector machines, decision trees, and classification algorithms. Rani and Kaushal [40] proposed an efficient network intrusion detection system based on the supervised machine learning technique of the random forest classifier and a minimum set of features extracted from the KDDCUP99 and NSLKDD datasets. This method yields 99.5% detection accuracy with little training time and effort required, as measured by these datasets. In order to improve upon traditional signature-based IDS methods, an anomaly-based IDS strategy that has been evaluated using the IoTID20 dataset [41]. This IDS method used a hybrid feature selection engine to narrow down the features to only those that are relevant to protecting IoT devices from unauthorized access. The random was trained and evaluated on the IoTID20 datasets. DDoS (99.95%), man-in-the-middle (MitM) (99.99%), and scanning (99.99%) assaults are all effectively detected by this study.

Table 3. Comparison for datasets (✓ = True, ✗ = False)

Dataset	Real Traffic	Label data	IoT traces	Zero-day attacks	Full packet captured	Year
DARPA 98	✓	✓	✗	✗	✓	1998
KDDCUP 99	✓	✓	✗	✗	✓	1999
CAIDA	✓	✗	✗	✗	✗	2007
NSL-KDD	✓	✓	✗	✗	✓	2009
ISCX 2012	✓	✓	✗	✗	✓	2012
ADFA-WD	✓	✓	✗	✓	✓	2017
ADFA-LD	✓	✓	✗	✓	✓	2018
CICIDS2017	✓	✓	✗	✓	✓	2019
BoT-IoT	✓	✓	✓	✓	✓	2020

#### 5. RESULTS AND DISCUSSION

Applying the concepts of set theory (intersection and union) to the issue of feature selection explains the result shown in Table 4. In this context, the presence of a characteristic in information gain (IG), and gain ratio (GR) techniques (or at least one of them) is indicative of the feature's greater relevance and non-redundancy. Multi-classification accuracy results for the IoTID20 dataset employing five distinct ML with different feature selection (FS) techniques are given in Table 5. Our proposed feature selection strategy improves the performance of ML classifiers, leading to the more appropriate classifications

(intersection mathematical set theory feature selection (IMF) and union mathematical set theory feature selection (UMF)).

The results of our hybrid FS technique for multi-classification issues on the IoTID20 dataset are displayed in Figure 6. There are five distinct ML models involved in this tactic, each of which is fused with a unique FS method. As can be shown in Table 5 and Figure 6, our proposed model uses ensemble to detect multi-classes with an accuracy of 99.70% utilizing either 11 or 28 features.

Table 4. Metrics for IoTID20's performance with a well curated feature set and ensemble

Feature	Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-Measure (%)	ROC Area (%)
60	IG-Ensemble	98.80	98.8	98.8	98.8	97.5
60	GR-Ensemble	98.74	98.7	98.7	98.7	97
20	IG-Ensemble	98.73	98.7	98.7	98.7	96.9
20	GR-Ensemble	98.56	98.6	98.6	98.6	95.5
28	UMF	98.98	98.9	98.9	98.9	98.9
11	IMF	98.98	98.9	98.9	98.9	98.9

Table 5. Multi-classification accuracy on the IoTID20 dataset using the five different ML and FS approaches

FS Approach Name	Classifiers Information Gain	Accuracy #	Classifiers Gain Ratio	Accuracy #	Classifiers Intersection	Accuracy #	Classifiers Union	Accuracy #
Model	IG-ANN	94.6	GR-ANN	93.86	IMF-ANN	92.8	ANN UMF	94
	IG-C.3.4	99.54	GR-C.3.4	99.1	IMF-C.3.4	99.59	C 4.5 UMF	99.6
	IG-Bagging	99.48	GR-Bagging	98.95	IMF-Bagging	99.58	Bagging UMF	99.6
	IG-kNN	98.48	GR-kNN	98.43	IMF-kNN	98.76	kNN UMK	99.1
	IG-Ensemble	99.6	GR-Ensemble	99.14	IMF-Ensemble	99.7	Ensemble UMF	99.7

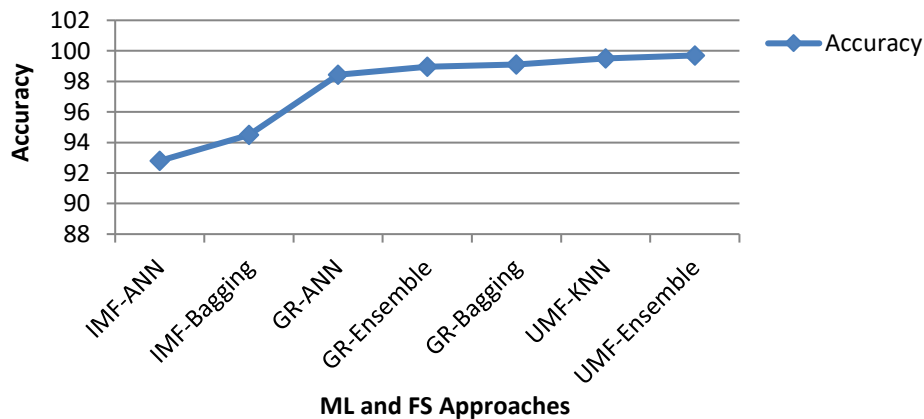


Figure 6. Multi-classification accuracy on the IoTID20 dataset using the five different ML and FS approaches

### 6. CONCLUSION

As a result of the internet of things capability of transforming items from a variety of application domains into Internet hosts, its adoption of connected devices has skyrocketed over the course of the last ten years across all spheres of human endeavor. At approximately the same time, vulnerabilities in the IoT put users' privacy and safety at risk. That is why it is critical to implement better IoT security measures immediately. When it comes to securing IoT networks, a machine-learning intrusion detection solution is a must-have. This research presents a summary of the techniques employed by IDSs to identify intrusions in IoT networks, all of which are based on machine learning. The following part of this research is a review of the many previous studies on this topic. Either an IDS strategy for IoT was detailed, or attack detection techniques for IoT were offered that could be implemented into IDS. In particular, this study described the authors' own implementations of various machine learning techniques that may be used for IDS on the internet of things. An assessment of the data sets currently available for investigating IoT safety is also provided. With an emphasis on intrusion detection using machine learning techniques, this study aims to provide academics with a synthesis of the many security challenges already encountered by IoT devices and networks.

## REFERENCES




- [1] A. Hameed and A. Alomary, "Security issues in IoT: a survey," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sep. 2019, pp. 1–5, doi: 10.1109/3ICT.2019.8910320.
- [2] X. Ma *et al.*, "A survey on deep learning empowered IoT applications," *IEEE Access*, vol. 7, pp. 181721–181732, 2019, doi: 10.1109/ACCESS.2019.2958962.
- [3] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhalaf, and H. Arshad, "A review on the security of the internet of things: challenges and solutions," *Wireless Personal Communications*, vol. 119, no. 3, pp. 2603–2637, Aug. 2021, doi: 10.1007/s11277-021-08348-9.
- [4] T. U. Sheikh, H. Rahman, H. S. Al-Qahtani, T. K. Hazra, and N. U. Sheikh, "Countermeasure of attack vectors using signature-based IDS in IoT environments," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct. 2019, pp. 1130–1136, doi: 10.1109/IEMCON.2019.8936231.
- [5] M. M. Noor and W. H. Hassan, "Current research on internet of things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.
- [6] G. R. Kumar, N. Mangathayaru, and G. Narsimha, "Intrusion detection a text mining based approach," *Arxiv.org/abs/1603.03837*, Mar. 2016.
- [7] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)," *Journal of ISMAC*, vol. 2, no. 4, pp. 190–199, Sep. 2020, doi: 10.36548/jismac.2020.4.002.
- [8] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based internet of things," *Procedia Manufacturing*, vol. 32, pp. 840–847, 2019, doi: 10.1016/j.promfg.2019.02.292.
- [9] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Applied Soft Computing*, vol. 72, pp. 79–89, Nov. 2018, doi: 10.1016/j.asoc.2018.05.049.
- [10] C. Lyu, X. Zhang, Z. Liu, and C.-H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for internet of things against DoS attack," *IEEE Access*, vol. 7, pp. 31068–31082, 2019, doi: 10.1109/ACCESS.2019.2902843.
- [11] N. Moustafa, K. K. R. Choo, I. Radwan, and S. Camtepe, "Outlier Dirichlet mixture mechanism: adversarial statistical learning for anomaly detection in the fog," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 1975–1987, 2019, doi: 10.1109/TIFS.2018.2890808.
- [12] A. Sagu and N. S. Gill, "Machine learning techniques for securing IoT environment," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 4, pp. 977–982, Feb. 2020, doi: 10.35940/ijitee.D1209.029420.
- [13] Y. Sei, J. A. Onesimu, and A. Ohsuga, "Machine learning model generation with copula-based synthetic dataset for local differentially private numerical data," *IEEE Access*, vol. 10, pp. 101656–101671, 2022, doi: 10.1109/ACCESS.2022.3208715.
- [14] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, N. Kumar, and Z. Han, "Sec-IoV: a multi-stage anomaly detection scheme for internet of vehicle," in *Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era*, Jul. 2019, pp. 37–42, doi: 10.1145/3331052.3332476.
- [15] J. M. Torres, C. Iglesias Comesaña, and P. J. García-Nieto, "Review: machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 10, pp. 2823–2836, Oct. 2019, doi: 10.1007/s13042-018-00906-1.
- [16] C. Ioannou and V. Vassiliou, "Classifying security attacks in IoT networks using supervised learning," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, May 2019, pp. 652–658, doi: 10.1109/DCOSS.2019.00118.
- [17] P. Illy, G. Kaddoum, C. Miranda Moreira, K. Kaur, and S. Garg, "Securing fog-to-things environment using intrusion detection system based on ensemble learning," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2019, pp. 1–7, doi: 10.1109/WCNC.2019.8885534.
- [18] D. H. Hoang and H. D. Nguyen, "Detecting anomalous network traffic in IoT networks," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, Feb. 2019, pp. 1143–1152, doi: 10.23919/ICACT.2019.8702032.
- [19] P. Manirih, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based intrusion detection approach for IoT networks using machine learning," in *2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, Nov. 2020, pp. 303–308, doi: 10.1109/CENIM51130.2020.9297958.
- [20] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, May 2020, doi: 10.1016/j.simpat.2019.102031.
- [21] R. Qaddoura, A. M. Al-Zoubi, I. Almomani, and H. Faris, "A multi-stage classification approach for IoT intrusion detection based on clustering with oversampling," *Applied Sciences*, vol. 11, no. 7, Mar. 2021, doi: 10.3390/app11073022.
- [22] M. Saravanan, A. M. Thoufeeq, S. Akshaya, and V. L. J. Manchari, "Exploring new privacy approaches in a scalable classification framework," in *2014 International Conference on Data Science and Advanced Analytics (DSAA)*, Oct. 2014, pp. 209–215, doi: 10.1109/DSAA.2014.7058075.
- [23] S. Papafotikas and A. Kakarountas, "A machine-learning clustering approach for intrusion detection to IoT devices," in *2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Sep. 2019, pp. 1–6, doi: 10.1109/SEEDA-CECNSM.2019.8908520.
- [24] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020, doi: 10.1109/ACCESS.2020.2994079.
- [25] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: a review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020, doi: 10.1016/j.procs.2020.04.133.
- [26] A. Shaver, Z. Liu, N. Thapa, K. Roy, B. Gokaraju, and X. Yuan, "Anomaly based intrusion detection for iot with machine learning," in *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, Oct. 2020, pp. 1–6, doi: 10.1109/AIPR50011.2020.9425199.
- [27] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, Jun. 2020, doi: 10.3390/app10124102.
- [28] 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, Oct. 2019, doi: 10.3390/electronics8111210.
- [29] K. Albulayhi and F. T. Sheldon, "An adaptive deep-ensemble anomaly-based intrusion detection system for the internet of things," in *2021 IEEE World AI IoT Congress (AIoT)*, May 2021, pp. 187–196, doi: 10.1109/AIIoT52608.2021.9454168.
- [30] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 924–935, Sep. 2019, doi: 10.1109/TNSM.2019.2927886.
- [31] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for






- detecting internet of things network attacks,” *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi: 10.1016/j.aej.2022.02.063.
- [32] H. Bostani and M. Sheikhan, “Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach,” *Computer Communications*, vol. 98, pp. 52–71, Jan. 2017, doi: 10.1016/j.comcom.2016.12.001.
- [33] Y. Feng, J. Zhong, C. Ye, and Z. Wu, “Clustering based on self-organizing ant colony networks with application to intrusion detection,” in *Sixth International Conference on Intelligent Systems Design and Applications*, Oct. 2006, vol. 2, pp. 1077–1080, doi: 10.1109/ISDA.2006.253761.
- [34] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for internet of things,” *Future Generation Computer Systems*, vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.
- [35] E. Anthi, L. Williams, and P. Burnap, “Pulse: an adaptive intrusion detection for the internet of things,” 2018, doi: 10.1049/cp.2018.0035.
- [36] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, “A scalable distributed machine learning approach for attack detection in edge computing environments,” *Journal of Parallel and Distributed Computing*, vol. 119, pp. 18–26, Sep. 2018, doi: 10.1016/j.jpdc.2018.03.006.
- [37] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, “A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks,” *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.
- [38] Y.-W. Chen, J.-P. Sheu, Y.-C. Kuo, and N. Van Cuong, “Design and implementation of IoT DDoS attacks detection system based on machine learning,” in *2020 European Conference on Networks and Communications (EuCNC)*, Jun. 2020, pp. 122–127, doi: 10.1109/EuCNC48522.2020.9200909.
- [39] T. Saba, T. Sadat, A. Rehman, Z. Mehmood, and Q. Javaid, “Intrusion detection system through advance machine learning for the internet of things networks,” *IT Professional*, vol. 23, no. 2, pp. 58–64, Mar. 2021, doi: 10.1109/MITP.2020.2992710.
- [40] D. Rani and N. C. Kaushal, “Supervised machine learning based network intrusion detection system for internet of things,” in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225340.
- [41] B. Susilo and R. F. Sari, “Intrusion detection in IoT networks using deep learning algorithm,” *Information*, vol. 11, no. 5, May 2020, doi: 10.3390/info11050279.

## BIOGRAPHIES OF AUTHORS






**Nisha**    received her BCA degree in computer science from Maharshi Dayanand University, Rohtak (Haryana), and received her MCA degree from Guru Gobind Singh Indraprastha University Delhi. She is a Ph.D. scholar at the Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India. She has qualified National Eligibility Test for assistant professor in India. She may be contacted at email: nisha.rs.dcsa@mdurohtak.ac.in.



**Nasib Singh Gill**    is currently head of Department of Computer Science and Applications, M.D. University, Rohtak, India. He is also working as Director, Directorate of Distance Education as well as director of digital learning center, M.D. University, Rohtak, Haryana. He earned his doctorate in computer science in the year 1996 and carried out his post-doctoral research at Brunel University, West London during 2001-2002. He is a recipient of the Commonwealth Fellowship Award of the British Government for the Year 2001. Besides, he also has earned his MBA degree. He is an active professional member of IETE, IAENG, and CSI. He has published more than 304 research papers and authored 5 popular books. He has guided so far 12 Ph.D. scholars as well as guiding about 5 more scholars. His research interests primarily include IoT, machine and deep learning, information and network security, data mining and data warehousing, NLP, and measurement of component-based systems. He can be contacted at email: nasib.gill@mdurohtak.ac.in.



**Preeti Gulia**    is currently working as an associate professor at the Department of Computer Science and Applications, M.D. University, Rohtak, India. She has been serving the Department since 2009. She earned her doctoral degree in 2013. She has published more than 65 research papers and articles in journals and conferences of National/International repute including ACM, and Scopus. Her area of research includes data mining, big data, machine learning, deep learning, IoT, and software engineering. She is an active professional member of IAENG, CSI, and ACM. She is also serving as an editorial board member active reviewer of international/national journals. She has guided four research scholars as well as guiding six Ph.D. research scholars from various research areas at present. She can be contacted at email: preeti@mdurohtak.ac.in.