Computer Systems Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.043107

ARTICLE

A Novel Intrusion Detection Model of Unknown Attacks Using Convolutional Neural Networks

Abdullah Alsaleh[1,2,*]

[1]Department of Information Engineering, Florence University, Florence, Italy

[2]Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Majmaah, Saudi Arabia

*Corresponding Author: Abdullah Alsaleh. Email: alsaleh@mu.edu.sa

Received: 21 June 2023 Accepted: 02 November 2023 Published: 19 March 2024

ABSTRACT

With the increasing number of connected devices in the Internet of Things (IoT) era, the number of intrusions is also increasing. An intrusion detection system (IDS) is a secondary intelligent system for monitoring, detecting and alerting against malicious activity. IDS is important in developing advanced security models. This study reviews the importance of various techniques, tools, and methods used in IoT detection and/or prevention systems. Specifically, it focuses on machine learning (ML) and deep learning (DL) techniques for IDS. This paper proposes an accurate intrusion detection model to detect traditional and new attacks on the Internet of Vehicles. To speed up the detection of recent attacks, the proposed network architecture developed at the data processing layer is incorporated with a convolutional neural network (CNN), which performs better than a support vector machine (SVM). Processing data are enhanced using the synthetic minority oversampling technique to ensure learning accuracy. The nearest class mean classifier is applied during the testing phase to identify new attacks. Experimental results using the AWID dataset, which is one of the most common open intrusion detection datasets, revealed a higher detection accuracy (94%) compared to SVM and random forest methods.

KEYWORDS

Internet of Vehicles; intrusion detection; machine learning; unknown attacks; data processing layer

1 Introduction

Over the past few decades, there has been a revolution in advanced computing and communication with smart devices. The Internet of Things (IoT) uses sensor devices to establish internal communication. IoT devices use the Internet as their primary communication medium, transferring large amounts of data over networks with minimal human intervention. Large-scale connectivity with different devices, unsecured network architectures and global data flow pose significant security challenges for IoT. Cyber security is an important concern in today's digital world to ensure protection from malicious activities aimed at dismantling organizational systems through data corruption, theft and unauthorized access. At the same time, IoT has become an important channel for the spread of dangerous malware attacks. Unsecured devices are targets for botnet operators to hijack systems and

control devices. Implementing a fully authenticated framework is essential to establish a strong security service that controls access mechanisms. The intrusion detection system (IDS) is a good way to address security problems and reducing the impact of attacks. IDS has become an integral part of network security management and host system security management. IDS recognizes networks or systems that are intruding or misused, reports them to administrators, and keeps records for further investigations. Handle suspicious events without disrupting normal activities during malicious outbreaks. There are many tools and techniques available to combat the threat of these attacks. The need for strong firewall protection is essential, as existing firewalls cannot classify behavior or anomalous attacks.

Open network architecture, heterogeneous device structures, and the widespread use of intelligent devices connected to our daily lives raise serious security and confidentiality concerns [1]. The destruction of industrial IoT water pumps, the theft of personal data [2], the creation of false messages as legitimate users [3], illegal control of power plants, intelligent cars, innovative restaurants and the manipulation of personal information to block scheduled services are some of the most recent dangers that have emerged in the IoT environment [4]. Therefore, comprehensive and well-defined security mechanisms are urgently needed to protect the digital world and prevent serious security threats [5]. This paper is organized as follows. Section 2 discusses the literature related to IDSs. Section 3 details the proposed model. Section 4 discusses the experiment and evaluation. Section 5 concludes this work and proposes future research directions.

2 Literature Review

An intrusion detection system monitors networks and uses conventional techniques to identify anomalous activity. Available IDS technologies lack dynamic attack detection against complex network structures. Probabilistic learning [6], fuzzy logic for dense attacks [7], analysis of risk factors by C4.5 decision tree algorithms [8], genetic methods [9], clustering [10], analysis of characteristics and their impact by regression [11] are some of the approaches used for intrusion detection models. All of these techniques are used to create robust or predictive or robust detection models based on data for actionable networks to prevent intruders and security breaches.

Recent research has experimented with eavesdropping, injection, and denial-of-service attacks. An intrusion prevention system (IPS) has been shown to be immune to these attacks [12]. Use the K-Means technique after outlier removal and integrate the local outlier coefficient (LOF) algorithm to evaluate scores that reflect observations anomalies. An automatic approximation-based tree automaton for security protocol analysis (TA4SP) uses a regular tree language to process intruder knowledge [13]. Nikhil et al. [14] proposed integrated agricultural forecasting and prevention techniques using linked devices. Real-time agricultural data from sensors were used and processed using machine learning (ML) and deep learning (DL) technologies. A convolutional neural network (CNN) was used with three sample animal images to train the model to avoid damage caused by physical encroachment on crops. USB camera inputs were compared to existing images using signature-based detection to trigger email notifications with alerts to avoid damage to the ecosystem [14]. Seo et al. proposed a two-step hybrid detection and prevention technique [15]. Evaluate decision trees for statistical analysis using the random forest method. If the ratio is less than zero, the packet is forwarded; otherwise, the packet is dropped. The best features analyzed in stage one move on to the next stage, where anomaly detection is implemented and traced to suspicious events and packets are dropped in stage two. Experiments are performed using datasets UNSW-NB15 and CICIDS2017. This model gives an accuracy of 99.80 at the second level of detection. Werth et al. [16] proposed layer-based prevention techniques that stimulate physical systems based on packet payloads. An additional contribution to this research

explores different threat models with consequences. Three layers were used; layer 0 for the physical device, layer 1 for the ladder program and layer 2 for activating the internal state of the ladder program. Changes in patterns within layers indicate malicious activity [16]. Hui Li et al. [17] proposed a model to minimize the error rate for improving performance in Snort-IDS. Combining this model with a firewall provides a high defense capability. There are numerous research applications for the security of IoT devices, including secured frameworks, data protection models and authentication technologies. Table 1 summarizes some of the recent studies on IDS.

Table 1: Some recent IDS studies

Item	Year	Strengths	limitations
[18]	2023	The selection of data pre-processing techniques for CAN ID, CAN Payload and CAN Frame are introduced.	High memory requirement to store all probabilities. Limited data pre-processing and ineffective feature selection for unsupervised learning.
[19]	2023	Discusses the importance of creating a secure ecosystem for the expanding market of electric vehicles and provides information on IDS for electric vehicle charging systems.	Does not provide an overview of all potential security risks associated with Internet-connected electric vehicle charging stations.
[20]	2023	Provides a detailed analysis of the importance of security in the context of electric vehicle charging stations and the IoT ecosystem.	Does not consider the use of deep learning techniques.
[21]	2023	Discusses a novel IDS based on vehicle voltage signals, which can effectively protect the security of in-vehicle networks.	Does not consider other related vehicle intrusion detection models.
[22]	2023	Presents a novel intrusion detection method for intra-vehicle networks using recurrence plots and neural networks.	Requires significant computational resources and expertise to implement and maintain.
[23]	2023	Provides information on a robust anomaly-based IDS for in-vehicle networks.	Does not provide information on the implementation of the proposed model in real-world scenarios.
[24]	2023	Provides a comprehensive survey of the current state of research on securing internal vehicle networks (IVNs) using deep learning techniques.	Does not provide details on datasets used to evaluate the performance.
[25]	2022	Provides a comprehensive approach to assessing security risks using hesitant fuzzy-sets.	Does not provide a detailed explanation of hesitant fuzzy-sets or the AHP-TOPSIS technique.

(Continued)

Table 1 (continued)

Item	Year	Strengths	limitations
[26]	2022	Provides valuable insights on cyber security analysis. It presents a detailed explanation of the AHP and technique for TOPSIS methods.	Shortage in achieving optimal outcomes.
[27]	2021	Provides a detailed explanation of a transfer learning-based intrusion detection scheme for the IoV. It proposes two model update schemes that utilize transfer learning to cope with new attacks in IoV.	Does not consider other approaches or techniques for intrusion detection in IoV.
[28]	2021	Presents a novel online auction mechanism that considers the unique attributes of EAVN, such as poor communication quality and various task demands.	Does not consider a comparison of the proposed auction mechanism with other existing auction mechanisms in the literature.
[29]	2020	Proposes a novel approach to edge caching in IoVs using multi-agent reinforcement learning.	Does not provide a detailed analysis of the computational and communication performance.
[30]	2023	The integration of neutrosophic sets and the Analytic Hierarchy Process (AHP) in addressing Multi-Criteria Decision Making (MCDM) issues.	Does not discuss the potential limitations or challenges of implementing the model in a real-world environment.
[31]	2023	Designs an adaptive memory auto encoder-based intrusion detection (AMAEID) model for in-vehicle message intrusion detection.	The size and diversity of the dataset are not illustrated.
[32]	2022	A comprehensive evaluation of the proposed approach using a large dataset of malware samples and benign files.	The lack of computational analysis.
[33]	2022	Provides a detailed study on the design and evaluation of one-dimensional editions of popular CNN architectures, including LeNet, VGG16, and ResNet, specifically tailored for analyzing ECG data.	Limited comparison with other approaches and preprocessing techniques.
[34]	2021	Addresses the healthcare sector's significant cybersecurity challenges and threats and provides a comprehensive overview of the challenges, threats, and solutions in securing the IoT in healthcare.	Does not discuss using machine learning and deep learning solutions for intrusion detection in healthcare systems.

(Continued)

Table 1 (continued)

Item	Year	Strengths	limitations
[35]	2020	Introduces the IntruDTree model, which reduces computational complexity by reducing feature dimensions.	The evaluation uses a limited number of security datasets.

Network attacks increase according to the development of applications related to the IoT. The literature presents network attack types that could be classified into two categories: (1) closed-set classification and (2) open-set classification.

2.1 Closed-Set Classification Method

Closed-set classification requires a predefined labeled dataset to detect intrusion. The authors in [36–38] detected attacks based on the matching issued from machine learning approaches. Yan et al. [39] combined the CNN method and the generative adversarial technique to follow the traces of intrusions. This method was evaluated using the KDDCUP'99 dataset and showed high accuracy. Roopak et al. [40] proposed CNN and long-short-term memory (LSTM) methods to identify IoT cyberattacks. The results of the proposals showed that the LSTM method performed better than the CNN method. Zhang et al. [41] attempted to benefit from CNN and LSTM methods. The authors modeled a deep hierarchical network and their experimental results showed better performance of their proposal compared to other network intrusion detection models in terms of accuracy. Louks et al. [42] used a neural network approach for IDS. Based on real-time data maintained during IoV operation, deep perceptron and recursive neural networks were performed. Vuong et al. [43] attempted to extract physical characteristics from IDS. Energy consumption and traffic features were considered when applying the decision tree-based method. Johes et al. [44] computed the error deviation of expected behavior to detect predicted attacks. Kang et al. [45] presented an unsupervised deep belief network technique. A deep neural network trains the issued probability vectors. These attempts belonging to closed-set classification did not support the detection of unknown intrusions in the test phase.

The detection of IDS attacks from the Vehicular Ad hoc Network (VANET) was carried out using a hybrid data-driven methodology by Hind Bangui et al. [46]. This methodology used a data-driven strategy to identify bad actors within the VANET network by merging many data models. The proposed hybrid data-driven model was validated by testing multiple environmental VANET systems. Alsarhan et al. [47] used a rule-based security filter to identify and remove anomalous nodes from the VANET network. The Dempster–Shafer theory was used for these refined nodes to draw out their linear qualities. To maximize the VANET system's detection rate, the authors put this rule-based anomaly-driven technique through its paces on a sizable real-time dataset. Many machine learning-based IDS systems were compared with the anomaly detection method to gauge its effectiveness in the VANET setting.

To better detect attackers in VANET, Vitalkar et al. [48] implemented a deep learning technique to improve the basic design of the IDS module. The primary goal of this endeavor was to develop methods for identifying attacks made between vehicle modules and roadside units. The authors used a deep learning system called Deep Belief Networks (DBNs) to identify assaults and used the CIC-IDS2017 dataset to verify their findings. Using a variety of categorization techniques, Alshammari et al. [49]

developed an innovative IDS module for VANET. Several validation strategies were applied to the complete experimental data. With the help of the machine learning technique and neural networks, Zeng et al. [50] were able to increase the efficiency of the performance of the VANET environment; the generated model's weighting bias and its various internal layers were examined. An IDS based on machine learning classifiers was developed by Shams et al. [51] to identify malicious network intrusions. As part of the VANET system, authors used a kernel-based SVM to categorize the IDSs that we already knew about from the ones we did not. However, when the number of vehicle nodes in the VANET system was large, this approach was unable to identify attacks.

Wattanapongsakorn et al. [52] presented a network-based IDS that detects known attack types and responds immediately. The suggested method was evaluated against an online network using various machine learning methods. The results reveal that the proposed IDPS can accurately distinguish normal occurrences from assaults within seconds and automatically block the victim's computer network from attacks. They also used the C4.5 Decision Tree technique to detect unknown attack types. However, the establishment of a strategy to detect unexpected and recognized threats could improve this study. Amaral et al. [53] suggested a wireless sensor network IDS enabled with IPv6, where traffic fingerprints and aberrant behaviors are used to identify assaults in the proposed system, which includes PPPSniffer and Finger2IPv6. The IDS locates network observers in the proposed system. Hence, neighbors' packets are monitored for attack attempts. The NIDS rules compare the observed messages, and a match triggers an alarm in the event management system. With this suggested approach, potential misbehaviors may be recognized instead of detecting predetermined assaults. The new detection rules enhanced the system. Kumar et al. [54] suggested and tested machine learning-based network IDSs to detect network threats. They built supervised machine learning classifiers that utilize labelled network traffic characteristics from benign and malicious apps. This study focused on Android-based malware due to the rise in mobile malware. The generated traffic was used to test the recommended technique, where premium SMS senders, backdoors, spammers, bots, ransomware, information stealers, and phony antivirus software generated the traffic. The suggested method detected unknown and known assaults with 99.4% accuracy. This work can be enhanced by extending the produced dataset and integrating it with the existing IDSs described. According to Qassim et al. [55], AIDS can identify malicious network traffic, alarming when it senses abnormal behavior. This study offered a strategy consisting of two parts. First, the authors recommended a collection of network traffic attributes that should be most useful for network anomaly detection. Second, a packet header-based anomaly detection method was presented to automatically categorize AIDS alarms. According to the authors, the suggested machine learning system is effective and efficient in recognizing harmful actions. This study may be enhanced by using other machine learning approaches to increase accuracy.

2.2 Open-Set Classification Method

The following approaches have been used to overcome the limits of closed-set classification methods by attempting to detect unknown attacks in the test phase.

Khan et al. [56] combined the anomaly detection model and the misuse detection model. The proposed enhanced scalability of hybrid IDS based on a convolutional long- and short-term memory network. Lin et al. [57] used the LSTM method to identify the abnormal network, with an attention mechanism supporting the technique. Gao et al. [58] constructed an IDS according to the extreme statistical values trained by the machine learning approach. Unfortunately, the findings have been proved only theoretically. Gou et al. [59] designed an IDS using a W-SVM classifier. The model was evaluated in the case of the KDDCUP'99 dataset. Hendricks et al. [60] tried to enhance intrusion

detection attacks by applying a deep learning approach, using the softmax probability as an indicator of classification. The unlabeled data were classified based on the softmax probability threshold. The authors in [61] and [62] proposed a pre-trained deep neural network according to temperature and perturbation features, aiming to distinguish between labeled and unlabeled samples on the softmax probability distribution. Shu et al. [63] predicted the source of pair samples when they were from the same or different classes using a deep pairwise classification network, and the unlabeled classes were defined according to the measured result of the distance metric. Hsu et al. [64] applied a model based on clustering objectives pairwise. Then, a training phase was performed on a deep clustering network.

The described attempts still suffered from the need for large data storage, time, cost, and training the learning model from scratch. To solve these shortcomings, the authors in [65] and [66] proposed CNN-based incremental learning to update the IDS model progressively. Then, the proposed method computes the nearest class. Li et al. [15] designed a transfer learning to update the IDS model based on a cloud-assisted scheme and a local update scheme.

According to the problems found in previous works, the proposed model belonging to the open-set classification method tries (1) to obtain more accurate results, and (2) to decrease the size of data. Table 2 shows some existing methods and their limitations, which were overcome by the proposed method.

Table 2: A comparison of some existing methods and their limitations

Distinctive characteristics	Limitations
Hybrid data-driven model [46]	Detected known attacks only
Features optimizations [47]	High detection time for attacks
Non-linear testing [48]	Complex detection algorithm
Robust algorithm [49]	Detected known attacks only
Required hardware [50]	Complex detection algorithm
Hybrid model [51]	Low sensitivity rate
Prevention system [52]	Detected known attacks only
IDS for IPv6 networks [53]	High detection time for attacks
Machine learning model [54]	Complex detection algorithm
Anomaly and network [55]	Detected known attacks only

2.3 Summarizing Important Studies

Several surveys are available in the scholarly literature. Table 3 summarizes some of the most important contributions from a selection of these works. It also provides a comprehensive contrast between the existing surveys and the new suggested work. These studies were compared in terms of their respective approaches to IoT security, discussion of distributed denial of service (DDoS) attacks, IDSs, study of IDS datasets, and IDS strategies based on machine and deep learning.

Table 3: A detailed comparison of some important surveys in IoT security domain

Article	IoT security issues	DDoS attacks discussion	Intrusion detection system	Database discussion for IDS	Machine learning techniques for IDS	Deep learning techniques for IDS
Subba et al. [67] 2016	√	√	√	×	√	×
Yang et al. [68] 2017	√	√	×	×	×	×
Yu et al. [69] 2017	√	×	√	×	×	×
Kouicem et al. [70] 2018	√	√	√	×	×	×
Frustaci et al. [71] 2018	√	√	√	×	×	×
Noor et al. [72] 2018	√	×	×	×	×	×
Chawla et al. [73] 2018	√	√	√	×	×	×
Deshpande et al. [74] 2018	√	×	√	×	×	×
Hassija et al. [75] 2019	√	√	√	×	√	×
Meneghello et al. [76] 2019	√	×	√	×	×	×
Byrnes et al. [77] 2020	√	√	×	×	×	×
Gassais et al. [78] 2020	√	×	×	×	×	×
Srivastava et al. [79] 2020	√	√	√	×	×	×
Anand et al. [80] 2020	√	√	×	×	√	×
Liu et al. [81] 2021	√	×	√	×	×	×
Park et al. [82] 2021	√	√	√	×	×	×
Proposed model	√	√	√	√	√	√

3 Proposed Model

This section provides background information about CNN, SVM and CAN. This section also describes the proposed model in detail.

3.1 Background

CAN plays a major role in the modern vehicle communication architecture. Messages transmitted through CAN show time relationships. In addition, CNN repeats the two convolution and pooling calculations alternately, whereas SVM is a learning method for linear discrimination functions in binary classification problems that achieve maximum margins. For example, when the accelerator pedals, more air enters the engine. The engine control unit senses the increase in airflow and then pumps more fuel into the engine to perform the necessary action. Consequently, the vehicle accelerates and the rotation per minute increases. These actions occur in a particular sequence and are converted into well-structured time sequences of traffic under normal driving conditions. However, when vehicles are abnormally affected by cyberattacks and faulty systems, the time relationship between messages observed in car networks may be different from these typical patterns. Conventional intrusion detection techniques in vehicular networks are based primarily on the temporal relationship between messages and their content. From a time point of view, many CAN messages are regular, which means that they usually appear at regular frequencies and show a sequence pattern. From a data point of view, the data content transferred by the CAN frame, which has the same CAN ID, also

shows certain patterns and trends under normal conditions. However, when a vehicle is cyber-attacked, the characteristics of these patterns change. On the one hand, DoS attacks in which attackers inject malicious messages into the network at high speeds affect the frequency and sequence of messages. However, integrity attacks in which malicious agents manipulate the data content affect the data models observed within CAN frameworks, although they may seem valid from a time perspective.

3.2 Description of the Proposed Model

Based on these established insights, we propose an accurate and fast IDS that supports an updating mechanism. The proposed architecture begins with a data collection phase. The road side unit (RSU) collects labeled and unlabeled data from the nearest vehicles as shown in Fig. 1, arrow 1. Then, unknown data are uploaded to the IoV cloud as illustrated in arrow 2. To accelerate the update model, the training is done in two layers: (1) an application service layer and (2) a data processing data layer. Response time, unbalanced datasets and false alarm rate are challenges that need to be addressed.

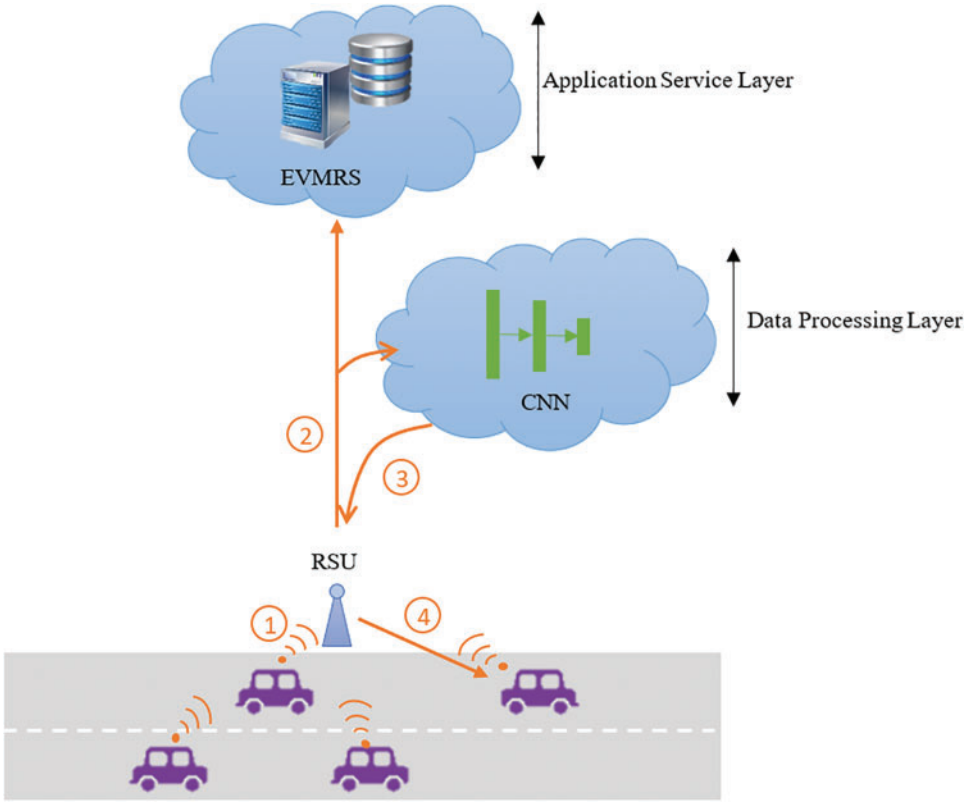

Figure 1: The proposed update model of the intrusion detection system

The first layer trains the new model with expert knowledge, and the second layer trains the new model with the provided data at an earlier time. After processing based on CNN training, the new models are loaded into the RSU as shown in arrow 3. The RSU deployed the new model to the target vehicle, arrow 4, when the accuracy of the arrived model, through the application service layer or data processing data, was above 85%. The proposed IDS architecture reveals the importance of the processing layer to ensure higher accuracy at the minimum required time.

This section focuses on the proposed network model based on open-set classification. The model is composed of three convolutional layers and a pooling layer. The classifier consists of the maximum mean discrepancy (MMD) and the cross-entropy (CE) [83] functions, as seen in Fig. 2.

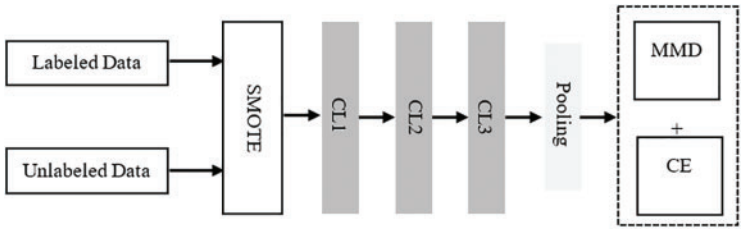

Figure 2: Training phase

The proposed model starts with augmenting the number of samples by applying the synthetic minority over-sampling technique (SMOTE) [84]. This technique is helpful in this case because of the imbalanced datasets. The SMOTE technique increases the sensitivity of the classifier to the minority class during the augmentation of datasets. It is added to the network model to overcome the issues cited by previous works related to the lack of labeled data.

The MMD function increases the distance between the characteristic distribution of labeled data and unlabeled data. Out-of-distribution data replace the unlabeled data during the training phase. The out-of-distribution data are generated by adding a small noise to the labeled data, as seen in Eq. (1).

$$D_{OD} = D + \varepsilon \tag{1}$$

where ε is the noise, D is the input data, and D_{OD} is the out-of-distribution data. The MMD is computed according to two distributions, as shown in Eq. (2).

$$D\,(LD, UD) = SupE_{LD}\,[f\,(D)] - E_{UD}\,[f\,(D_{OD})] \tag{2}$$

where E_{LD} is the dataset of labeled data, and the E_{UD} is the dataset of unlabeled data. The CE function measures the probability difference between two distributions. Eq. (3) describes the CE function.

$$H\,(P_{LD} - Q_{UD}) = -\sum P_{LD}\,[f\,(D)] \times \log(Q_{UD}\,[f\,(D_{OD})]) \tag{3}$$

where P_{LD} is the probability related to the labeled data, and Q_{UD} is the probability related to the unlabeled data. During the training phase, the loss L is computed in every iteration t based on Eq. (4).

$$\frac{\partial L^t}{\partial f_i^t} = \frac{\partial L_{CE}^t}{\partial f_i^t} + \delta \frac{\partial L_{MMD}^t}{\partial f_i^t} \tag{4}$$

The neural network parameters W are updated when the convergence is achieved using Eq. (5).

$$W^{t+1} = W^t - LR \times \sum\nolimits_{i=1}^{n} \frac{\partial L^t}{\partial f_i^t} \frac{\partial f_i^t}{\partial W^t} \tag{5}$$

where LR is the learning rate. In the testing phase, the achieved IDS model is evaluated by the Deep Nearest Class Mean (DNCM) [85] classifier, as shown in Fig. 3.

The DNCM classifier provides an improved method to directly learn nonlinear deep features of the data. Eq. (6) describes the DNCM method.

$$y = argmind(x_{LD}, x_{UD}) \tag{6}$$

where d is the Euclidean distance. Samples that are farther from the nearest known class are more likely to be in the unknown class. Data are classified as the unknown class if the associated distance from the test sample to its nearest class mean is greater than the corresponding class.

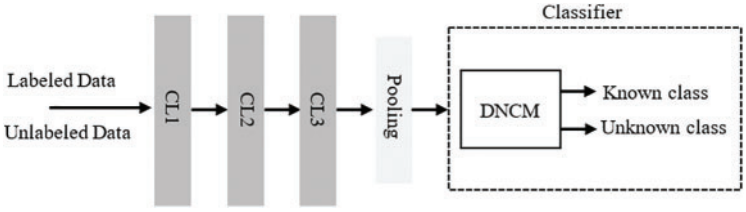

Figure 3: Training phase

4 Experiment and Evaluation

The evaluation of the proposed model is performed on Windows 10 with a 64-bit system, a core i7 processor and 8 gigabytes of memory. The Python 3 language is used for environment development. The Scikit learning library is called to ensure the machine learning phase. The data processing is supported by Weka software. The AWID dataset [86] is used to validate the proposed network architecture and the IDS model. The AWID wireless network security is a relatively new dataset in which new attack types are more realistic. It is an open-source dataset and is widely used for contribution evaluation.

To highlight the effectiveness of the proposed IDS scheme, its accuracy, detection rate (DR), false alarm rate (FAR), and false negative rate (FNR) metrics are compared with those of the support vector machine (SVM) algorithm used by Cruz et al. [87] and the random forest (RF) algorithm used by Yalin et al. [88]. We mention that these algorithms are adapted according to the AWID dataset. These two methods were the more significant methods in the case of open-set classification methods. The MMD function used in our scheme computes the differences between normal and abnormal features of the network traffic.

The experiments shown in Fig. 4 prove the importance of the MMD algorithm. The drawn results reveal that the distribution of the data is similar when the attack types are the same. The MMD distance between (dist1, dist2) and the distance between (dist3, dist4) are minimal because both pairs belong to the same network domain. Therefore, a network attack is detected when the MMD measurement related to the traffic feature is significant.

The above findings prove the need for an accurate intrusion detection model to support new types of attacks. To evaluate the accuracy of the IDS-based machine learning and traditional methods based on SVM and RF, this paper focuses on three main types of attacks: impersonation attack, flooding attack, and injection attack as shown in Table 4.

Very important metrics are used to measure and compare the performance of the proposed model against the well-known IDSs presented in [87] and [88]. Table 5 summarizes the performance of the compared models. According to Figs. 5a–5c, the results related to the proposed IDS model are better than those of SVM and RF. The suggested IDS model has an average accuracy of about 94% compared to SVM at about 86% and RF at about 89%. From the detection rate curves, it can be seen that the proposed method achieved the full rate. The average false alarm rate is nearly 3%, ensuring the reliability of the proposed machine learning model. On the basis of the false negative rate curves, the proposed model performed better than SVM and RF, but still requires enhancement.

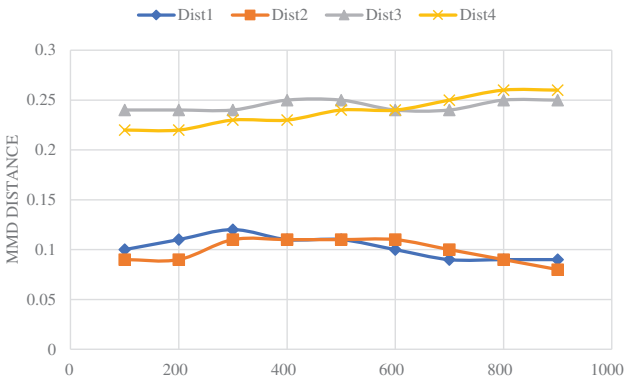

Figure 4: MMD difference between on-data distribution

Table 4: AWID dataset analysis of class distribution

Attack type	Count
Impersonation	1884378
Flooding	1211459
Injection	1530373

Table 5: Summary of models performance

Item	Accuracy	Detection rate	False alarm rate	False negative rate
Cruz et al. [87]	86%	81%	29%	9%
Yalin et al. [88]	89%	90%	16%	5%
Proposed model	94%	100%	3%	4%

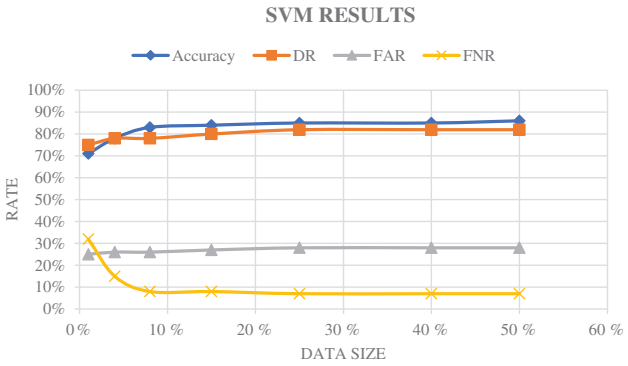

Figure 5(a): SVM

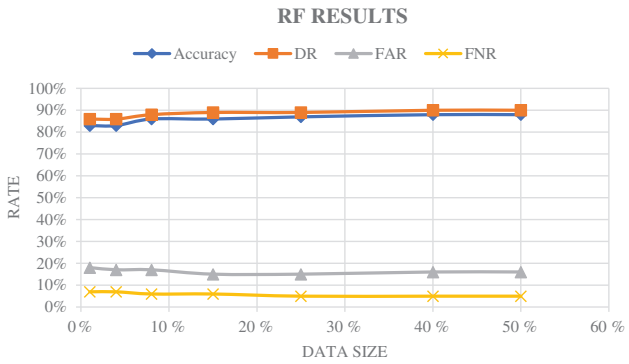

Figure 5(b): RF

Figure 5(c): Proposed model

The results the effectiveness of the proposed model, which reached a higher detection accuracy compared with the traditional machine learning scheme even when a small amount of target domain is used. Fig. 5c shows that when only 4% of the data in the source domain is used, the accuracy, DR, and FNR of the proposed model are higher than those of other schemes. The communication and the time overhead are reduced. Therefore, the proposed IDS model-based machine learning ensures effectiveness and accuracy with a lower time cost.

5 Conclusion

As the number of IoT devices, users, services and applications continues to grow, there is an increasing necessity for a reliable and effective security resolution that is appropriate for usage in IoT settings. Additionally, since IoT networks serve as the foundation for smart settings, any flaws in their safety have a direct impact on the smart environments in which they are built. Attacks like denial of service (DoS), distributed denial of service (DDoS), probing and RPL occurrences hurt the services and applications available in IoT-based smart settings. As a result, the security of IoT settings is a very significant concern. An IDS is one potential solution to this problem. This paper provides a review of IDSs intended for IoT settings. Recommendations for developing an IDS that is both robust and lightweight were also given. In this work, several articles were examined that were primarily concerned with the design and implementation of IDSs for use in the IoT paradigm, which may be used in smart environments. The characteristics of all IDS techniques described in these articles were enumerated and discussed. In addition, this paper provides several suggestions for the consideration of different

aspects when designing IoT IDS, such as the need for a powerful system with a lightweight positioning strategy that does not negatively impact the integrity and availability of the IoT environment. Based on the diverse research findings, an integrated IDS that may be used in IoT-based smart settings is required to effectively address closed-set classification and open-set classification of data. With the increasing use of IoV-type attacks and the large need to ensure the safety of network traffic, this paper provides an accurate IDS based on specific machine learning methods. The proposed model deploys a convolutional neural network in the data processing layer and the success of the proposal could be summarized as follows: (1) the SMOTE technique is used to broaden the dataset samples, (2) the MMD function augments the distance between labeled and unlabeled data features, and (3) the DNCM classifies the data deeply in the testing phase. The simulation results based on the AWID dataset prove that the proposed architecture and IDS model reached an accuracy of around 94% even with a small data size.

Acknowledgement: Not applicable.

Funding Statement: The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2024-920).

Author Contributions: Study conception and design: Abdullah Alsaleh; data collection: Abdullah Alsaleh; analysis and interpretation of results: Abdullah Alsaleh; draft manuscript preparation: Abdullah Alsaleh. The author reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated and/or analyzed during the current study are available in the Aegean repository, https://icsdweb.aegean.gr/awid/download-dataset.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Carvalho and J. Granjal, "Security and privacy for mobile IoT applications using blockchain," *Sensors*, vol. 21, no. 17, pp. 5931–5952, 2021.

[2] S. Singh, P. K. Sharma, S. Y. Moon and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2017. https://doi.org/10.1007/s12652-017-0494-4

[3] B. Yuan, Y. Jia, L. Xing, D. Zhao, X. Wang *et al.,* "Shattered chain of trust: Understanding security risks in cross-cloud IoT access delegation," in *Proc. of 29th USENIX Secur. Symp. (USENIX Security)*, pp. 1183–1200, 2020.

[4] T. Alladi, V. Chamola, B. Sikdar and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[5] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi *et al.,* "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Computer Networks*, vol. 177, 2020. https://doi.org/10.1016/j.comnet.2020.107333

[6] M. C. J. Sekhar, K. Tulasi, V. V. Amulya, D. R. Teja and M. S. Kumar, "Implementation of IDS using snort on Bayesian network," *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 4, pp. 790–795, 2015.

[7] R. Shanmugavadivu and N. Nagarajan, "Network intrusion detection system using fuzzy logic," *Indian Journal of Computer Science and Engineering*, vol. 2, no. 1, pp. 101–111, 2011.

[8] K. Rai, M. S. Devi and A. Guleria, "Decision tree based algorithm for intrusion detection," *International Journal of Advanced Networking and Applications*, vol. 7, no. 4, pp. 2828–2834, 2016.

[9] M. S. Hoque, Md. Mukit and Md. A. Bikas, "An implementation of intrusion detection system using genetic algorithm," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, pp. 109–120, 2012.
[10] M. V. Rao, A. Damodaram and N. C. B. Charyulu, "Algorithm for clustering with intrusion detection using modified and hashed K-Means algorithm," in *Advances in Computer Science Engineering & Applications*, vol. 167. Berlin, Heidelberg, Springer, pp. 737–744, 2012. https://doi.org/10.1007/978-3-642-30111-7_70
[11] X. Bao, T. Xu and H. Hou, "Network intrusion detection based on support vector machine," in *2009 Int. Conf. Management and Service Science*, Beijing, China, pp. 1–4, 2009. https://doi.org/10.1109/ICMSS.2009.5304051
[12] T. Alves, R. Das and T. Morris, "Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers," *IEEE Embedded Systems Letters*, vol. 10, no. 3, pp. 99–102, 2018.
[13] P. R. Chandre, P. N. Mahalle and G. R. Shinde, "Machine learning based novel approach for intrusion detection and prevention system: A tool based verification," in *IEEE Global Conf. on Wireless Computing and Networking (GCWCN)*, Lonavala, India, pp. 135–140, 2018. https://doi.org/10.1109/GCWCN.2018.8668618
[14] R. Nikhil, B. S. Anisha and P. R. Kumar, "Real-time monitoring of agricultural land with crop prediction and animal intrusion prevention using Internet of Things and machine learning at edge," in *IEEE Int. Conf. on Electronics, Computing and Communication Technologies (CONECCT)*, Bangalore, India, pp. 1–6, 2020. https://doi.org/10.1109/CONECCT50063.2020.9198508
[15] W. Seo and W. Pak, "Real-time network intrusion prevention system based on hybrid machine learning," *IEEE Access*, vol. 9, pp. 46386–46397, 2021. https://doi.org/10.1109/ACCESS.2021.3066620
[16] A. Werth and T. H. Morris, "A specification-based intrusion prevention system for malicious payloads," *Advances in Intelligent Systems and Computing*, vol. 1055, pp. 153–168, 2020. https://doi.org/10.1007/978-3-030-31239-8_13
[17] H. Li and D. Liu, "Research on intelligent intrusion prevention system based on snort," in *Int. Conf. on Computer, Mechatronics, Control and Electronic Engineering (CMCE)*, Changchun, China, pp. 251–253, 2010. https://doi.org/10.1109/CMCE.2010.5610483
[18] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo *et al.,* "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–40, 2023.
[19] M. ElKashlan, H. Aslan, M. S. Elsayed, A. D. Jurcut and M. A. Azer, "Intrusion detection for electric vehicle charging systems (EVCS)," *Algorithms*, vol. 16, no. 2, pp. 75–86, 2023.
[20] M. ElKashlan, M. S. Elsayed, A. D. Jurcut and M. Azer, "A Machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs)," *Electronics*, vol. 12, no. 4, pp. 1044–1060, 2023.
[21] Y. Xun, Z. Deng, J. Liu and Y. Zhao, "Side channel analysis: A novel intrusion detection system based on vehicle voltage signals," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 7240–7250, 2023.
[22] O. Y. Al-Jarrah, K. E. Haloui, M. Dianati and C. Maple, "A novel detection approach of unknown cyber-attacks for intra-vehicle networks using recurrence plots and neural networks," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 271–280, 2023. https://doi.org/10.1109/OJVT.2023.3237802
[23] J. Xiao, L. Yang, F. Zhong, H. Chen and X. Li, "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework," *Applied Intelligence*, vol. 53, pp. 3183–3206, 2023. https://doi.org/10.1007/s10489-022-03412-8
[24] B. Lampe and W. Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Systems with Applications*, vol. 221, pp. 119771–119793, 2023. https://doi.org/10.1016/j.eswa.2023.119771
[25] A. S. Alfakeeh, A. Almalawi, F. J. Alsolami, Y. B. Abushark, A. I. Khan *et al.,* "Hesitant fuzzy-sets based decision-making model for security risk assessment," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2297–2317, 2022.

[26] Y. B. Abushark, A. I. Khan, F. Alsolami, A. Almalawi, M. M. Alam *et al.,* "Cyber security analysis and evaluation for intrusion detection systems," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1765–1783, 2022.
[27] X. Li, Z. Hu, M. Xu, Y. Wang and J. Ma, "Transfer learning based intrusion detection scheme for Internet of Vehicles," *Information Sciences*, vol. 547, pp. 119–135, 2021. https://doi.org/10.1016/j.ins.2020.05.130
[28] X. Peng, K. Ota, M. Dong and H. Zhou, "Online resource auction for EAVN with non-price attributes," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7127–7137, 2021.
[29] K. Jiang, H. Zhou, D. Zeng and J. Wu, "Multi-agent reinforcement learning for cooperative edge caching in Internet of Vehicles," in *2020 IEEE 17th Int. Conf. on Mobile Ad Hoc and Sensor Systems (MASS)*, Delhi, India, pp. 455–463, 2020. https://doi.org/10.1109/MASS50613.2020.00062
[30] A. Sleem and I. Elhenawy, "An interval valued neutrosophic sets integrated with the AHP MCDM methodology to assess the station of 5G network," *Journal of Neutrosophic and Information Fusion*, vol. 1, no. 1, pp. 34–40, 2023.
[31] P. Wei, B. Wang, X. Dai, L. Li and F. He, "A novel intrusion detection model for the CAN bus packet of in-vehicle network based on attention mechanism and autoencoder," *Digital Communications and Networks*, vol. 9, no. 1, pp. 14–21, 2023.
[32] A. Abdelmonem and S. S. Mohamed, "Deep learning defenders: Harnessing convolutional networks for malware detection," *Journal of International Journal of Advances in Applied Computational Intelligence*, vol. 1, no. 2, pp. 46–55, 2022. https://doi.org/10.54216/IJAACI.010203
[33] A. S. Aziz, H. K. Mohamed and A. Abdelhafeez, "Unveiling the power of convolutional networks: Applied computational intelligence for arrhythmia detection from ECG signals," *Journal of International Journal of Advances in Applied Computational Intelligence*, vol. 1, no. 2, pp. 63–72, 2022.
[34] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis *et al.,* "A self-learning approach for detecting intrusions in healthcare systems," in *ICC 2021—IEEE Int. Conf. on Communications*, Montreal, QC, Canada, pp. 1–6, 2021. https://doi.org/10.1109/ICC42927.2021.9500354
[35] I. H. Sarker, Y. B. Abushark, F. Alsolami and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, pp. 754–768, 2020.
[36] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Computer Communications*, vol. 49, pp. 1–17, 2014. https://doi.org/10.1016/j.comcom.2014.04.012
[37] M. Agarwal, D. Pasumarthi, S. Biswas and S. Nandi, "Nandi machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization," *International Journal of Machine Learning and Cybernetics*, vol. 7, pp. 1035–1051, 2016. https://doi.org/10.1007/s13042-014-0309-2
[38] R. A. R. Ashfaq, Y. He and D. Chen, "Toward an efficient fuzziness based instance selection methodology for intrusion detection system," *International Journal of Machine Learning and Cybernetics*, vol. 8, pp. 1767–1776, 2017. https://doi.org/10.1007/s13042-016-0557-4
[39] Q. Yan, M. Wang, W. Huang, X. Luo and F. R. Yu, "Automatically synthesizing DoS attack traces using generative adversarial networks," *International Journal of Machine Learning and Cybernetics*, vol. 10, pp. 3387–3396, 2019. https://doi.org/10.1007/s13042-019-00925-6
[40] M. Roopak, G. Yun Tian and J. Chambers, "Deep learning models for cyber security in IoT networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conf. (CCWC)*, Las Vegas, NV, USA, pp. 0452–0457, 2019. https://doi.org/10.1109/CCWC.2019.8666588
[41] Y. Zhang, X. Chen, L. Jin, X. Wang and D. Guo, "Network intrusion detection: Based on deep hierarchical network and original flow data," *IEEE Access*, vol. 7, pp. 37004–37016, 2019. https://doi.org/10.1109/ACCESS.2019.2905041
[42] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon *et al.,* "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018. https://doi.org/10.1109/ACCESS.2017.2782159
[43] T. P. Vuong, G. Loukas and D. Gan, "Performance evaluation of cyber-physical intrusion detection on a robotic vehicle," in *2015 IEEE Int. Conf. on Computer and Information Technology; Ubiquitous Computing*

and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, pp. 2106–2113, 2015. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.313

[44] A. Jones and J. Straub, "Using deep learning to detect network intrusions and malware in autonomous robots," *Cyber Sensing*, vol. 10185, pp. 1018505–1018511, 2017. https://doi.org/10.1117/12.2264072

[45] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, 2016. https://doi.org/10.1371/journal.pone.0155781

[46] H. Bangui, M. Ge and B. Buhnova, "A hybrid data-driven model for intrusion detection in VANET," *Procedia Computer Science*, vol. 184, pp. 516–523, 2021. https://doi.org/10.1016/j.procs.2021.03.065

[47] A. Alsarhan, A. R. Al-Ghuwairi, I. T. Almalkawi, M. Alauthman and A. Al-Dubai, "Machine learning-driven optimization for intrusion detection in smart vehicular networks," *Wireless Personal Communications*, vol. 117, no. 4, pp. 3129–3152, 2021.

[48] R. S. Vitalkar, S. S. Thorat and D. V. Rojatkar, "Intrusion detection for vehicular Ad Hoc network based on deep belief network," In: S. Smys, R. Bestak, R. Palanisamy, I. Kotuliak (Eds.), *Computer Networks and Inventive Communication Technologies*, pp. 853–865, Singapore: Springer, 2022. https://doi.org/10.1007/978-981-16-3728-5_64

[49] A. Alshammari, M. A. Zohdy, D. Debnath and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wireless Engineering and Technology*, vol. 9, no. 4, pp. 79–94, 2018.

[50] Y. Zeng, M. Qiu, Z. Ming and M. Liu, "Senior2Local: A machine learning based intrusion detection method for VANETs," In: M. Qiu (Ed.), *Smart Computing and Communication*, Cham: Springer, pp. 417–426, 2018. https://doi.org/10.1007/978-3-030-05755-8_41

[51] E. A. Shams, A. Rizaner and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Computers & Security*, vol. 78, pp. 245–254, 2018. https://doi.org/10.1016/j.cose.2018.06.008

[52] N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom *et al.,* "A practical network-based intrusion detection and prevention system," in *2012 IEEE 11th Int. Conf. on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, pp. 209–214, 2012. https://doi.org/10.1109/TrustCom.2012.46

[53] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han and L. Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," in *2014 IEEE Int. Conf. on Communications (ICC)*, Sydney, NSW, Australia, pp. 1796–1801, 2014. https://doi.org/10.1109/ICC.2014.6883583

[54] S. Kumar, A. Viinikainen and T. Hamalainen, "Machine learning classification model for network based intrusion detection system," in *2016 11th Int. Conf. for Internet Technology and Secured Transactions (ICITST)*, Barcelona, Spain, pp. 242–249, 2016. https://doi.org/10.1109/ICITST.2016.7856705

[55] Q. Qassim, A. M. Zin and M. J. A. Aziz, "Anomalies classification approach for network-based intrusion detection system," *International Journal of Network Security*, vol. 18, no. 6, pp. 1159–1172, 2016.

[56] M. A. Khan, M. Karim and Y. Kim, "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network," *Symmetry*, vol. 11, no. 4, pp. 583–596, 2019.

[57] P. Lin, K. Ye and C. Z. Xu, "Dynamic network anomaly detection system by using deep learning techniques," in *Cloud Computing–CLOUD 2019*, vol. 11513, pp. 161–176, 2019. https://doi.org/10.1007/978-3-030-23502-4_12

[58] F. Gao, H. Yoon, T. Wu and X. Chu, "A feature transfer enabled multi-task deep learning model on medical imaging," *Expert Systems with Applications*, vol. 143, pp. 112957–112987, 2020. https://doi.org/10.1016/j.eswa.2019.112957

[59] S. Gou, Y. Wang, L. Jiao, J. Feng and Y. Yao, "Distributed transfer network learning based intrusion detection," in *2009 IEEE Int. Symp. on Parallel and Distributed Processing with Applications*, Chengdu, China, pp. 511–515, 2009. https://doi.org/10.1109/ISPA.2009.92

[60] D. Hendrycks and K. Gimpel, "A baseline for detecting misclassified and out-of-distribution examples in neural networks," 2016. https://doi.org/10.48550/arXiv.1610.02136

[61] S. Liang, Y. Li and R. Srikant, "Enhancing the reliability of out-of-distribution image detection in neural networks," 2017. https://doi.org/10.48550/arXiv.1706.02690

[62] K. Shmelkov, C. Schmid and K. Alahari, "Incremental learning of object detectors without catastrophic forgetting," in *Proc. of the IEEE Int. Conf. on Computer Vision*, Venice, Italy, pp. 3400–3409, 2017. https://doi.org/10.48550/arXiv.1708.06977
[63] L. Shu, H. Xu and B. Liu, "Unseen class discovery in open-world classification," 2018. https://doi.org/10.48550/arXiv.1801.05609
[64] Y. C. Hsu, Z. Lv, J. Schlosser, P. Odom and Z. Kira, "Kira A probabilistic constrained clustering for transfer learning and image category discovery," 2018. https://doi.org/10.48550/arXiv.1806.11078
[65] S. A. Rebuffi, A. Kolesnikov, G. Sperl and C. H. Lampert, "ICaRL: Incremental classifier and representation learning," in *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, Honolulu, HI, USA, pp. 2001–2010, 2017. https://doi.org/10.48550/arXiv.1611.07725
[66] D. J. Sutherland, H. Tung, H. Strathmann, S. De, A. Ramdas *et al.,* "Generative models and model criticism via optimized maximum mean discrepancy," 2016. https://doi.org/10.48550/arXiv.1611.04488
[67] B. Subba, S. Biswas and S. Karmakar, "A neural network based system for intrusion detection and attack classification," in *2016 Twenty Second National Conf. on Communication (NCC)*, Guwahati, India, pp. 1–6, 2016. https://doi.org/10.1109/NCC.2016.7561088
[68] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.
[69] W. Yu, F. Liang, X. He, W. Hatcher, C. Lu *et al.,* "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018. https://doi.org/10.1109/ACCESS.2017.2778504
[70] D. E. Kouicem, A. Bouabdallah and H. Lakhlef, "Internet of Things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018. https://doi.org/10.1016/j.comnet.2018.03.012
[71] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.
[72] M. Noor and W. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019. https://doi.org/10.1016/j.comnet.2018.11.025
[73] S. Chawla and T. Geethapriya, "Security as a service: Real-time intrusion detection in Internet of Things," in *Proc. of the Fifth Cybersecurity Symp.*, Coeur d' Alene, Idaho, pp. 1–4, 2018. https://dl.acm.org/doi/abs/10.1145/3212687.3212872
[74] C. Troeger, B. F. Blacker, I. A. Khalil, P. C. Rao, S. Cao *et al.,* "Estimates of the global, regional, and national morbidity, mortality, and aetiologies of diarrhoea in 195 countries: A systematic analysis for the Global Burden of Disease Study 2016," *Lancet Infect Diseases*, vol. 18, no. 11, pp. 1211–1228, 2018.
[75] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal *et al.,* "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019. https://doi.org/10.1109/ACCESS.2019.2924045
[76] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.
[77] S. Wu, B. Daragh and W. Molly, "Megereality: Leveraging physical affordances for multi-device gestural interaction in augmented reality," in *Extended Abstracts of the 2020 CHI Conf. on Human Factors in Computing Systems*, Honolulu, HI, USA, pp. 1–4, 2020. https://doi.org/10.1145/3334480.3383170
[78] R. Gassais, J. M. Fernandez, D. Aloise and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of Things," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–16, 2020.
[79] M. Saharkhizan, A. Azmoodeh, H. HaddadPajouh, A. Dehghantanha, R. M. Parizi *et al.,* "A Hybrid deep generative local metric learning method for intrusion detection," In: K. K. Choo, A. Dehghantanha (Eds.), *Handbook of Big Data Privacy*, Cham: Springer, pp. 343–357, 2020. https://doi.org/10.1007/978-3-030-38557-6_16
[80] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar *et al.,* "IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges," *IEEE Access*, vol. 8, pp. 168825–168853, 2020. https://doi.org/10.1109/ACCESS.2020.3022842

[81] Y. Cui, F. Liu, X. Jing and J. Mu, "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," *IEEE Network*, vol. 35, no. 5, pp. 158–167, 2021.
[82] W. Choi, J. Kim, S. Lee and E. Park, "Smart home and internet of things: A bibliometric study," *Journal of Cleaner Production*, vol. 301, pp. 126908, 2021. https://doi.org/10.1016/j.jclepro.2021.126908
[83] R. Y. Rubinstein and D. P. Kroese, *The Cross-Entropy Method: A Unified Approach to Combinatorial Optimization, Monte-Carlo Simulation and Machine Learning*, Berlin, Heidelberg: Springer Science & Business Media, 2013.
[84] N. V. Chawla, K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002. https://doi.org/10.1613/jair.953
[85] S. Guerriero, B. Caputo and T. Mensink, "Deepncm: Deep nearest class mean classifiers," in *ICLR 2018 Workshop*, Vancouver, BC, Canada, 2018. https://openreview.net/pdf?id=rkPLZ4JPM
[86] P. Satam and S. Hariri, "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 1077–1091, 2021.
[87] S. Cruz, C. Coleman, E. M. Rudd and T. E. Boult, "Open set intrusion recognition for fine-grained attack categorization," in *2017 IEEE Int. Symp. on Technologies for Homeland Security (HST)*, Waltham, MA, USA, pp. 1–6, 2017. https://doi.org/10.1109/THS.2017.7943467
[88] Y. L. Li, F. Li and J. Q. Song, "The research of random forest intrusion detection model based on optimization in Internet of Vehicles," *Journal of Physics: Conference Series*, vol. 1757, no. 1, pp. 012149–012158, 2021.