CNN-KPCA: A hybrid Convolutional Neural Network with Kernel Principal Component Analysis for Intrusion Detection System for the Internet of Things Environments

Joseph Bamidele Awotunde[1], Ranjit Panigrahi[2], Biswajit Brahma[3] and Akash Kumar Bhoi[4]

[1] *Department of Computer Science, University of Ilorin, Ilorin, Nigeria*
[2] *Department of Computer Applications, Sikkim Manipal Institute of Technology, Sikkim Manipal University, Sikkim, India*
[3] *McKesson Corporation, 1 Post St, San Francisco, CA 94104, USA*
[4] *Directorate of Research, Sikkim Manipal University, Gangtok, Sikkim, India*

Abstract

The combination of several Machine Learning and Deep Learning techniques has been spurred by the need to address security breaches inside an Internet of Things (IoT) focused environment. This research presents a novel way to solve the challenge of classifying normal and abnormal attacks on the Domain Name System (DNS) protocol. The proposed method involves the use of a hybrid model that combines Convolutional Neural Networks (CNN) with Principal Component Analysis (PCA). The methodology begins by transforming nominal features into numerical data as part of the preprocessing stage. The quantitative data is subsequently subjected to PCA in order to identify features, reducing the dimensions of the dataset by separating the most important properties. Following this, the data is inputted into the CNN with the objective of detecting and categorizing anomalous behaviors inside the IoT ecosystem. The effectiveness of the hybrid model was assessed by employing the IoTID20 dataset. The model exhibited exceptional performance in terms of accuracy, recall, F-Score, precision, and ROC metrics, surpassing those of existing detection methods. Significantly, the suggested framework not only improves security measures but also tackles privacy concerns and strengthens the maintainability of IoT-based systems.

Keywords

Machine learning, Deep learning, Principal component analysis, Convolutional neural network, Intrusion detection [1]

1. Introduction

The eventual convergence of cutting-edge sensor technology and the Internet of Things (IoT), quickly infiltrating human existence, is unavoidable. The number of linked things on the Internet will have surpassed 50 billion by 2020 [1], [2]. Data Streams are usually dynamic, such as in time-series format, and their memory consumption and processing time are constrained by hardware and database server limits [3]. Because they use centralized and broadened operating systems, IT infrastructure, and applications, IoT-based systems are defenceless against traditional threats. On the other hand, traditional cloud computing risks face new security concerns due to several technological advancements that could lead to new types of misuse [4]. Network Intrusion Detection Systems (IDSs) are now essential for restoring network security, especially for IoT-based systems [4]–[6]. Because of the complexity and heterogeneity of these systems, it isn't easy to find a haven for them from cyber-attacks [7]. Furthermore, having different types of operators necessitates varying levels of protection.

The loss of control over the infrastructure used by Cloud customers is one of the most serious issues they face [8]. High missing and noisy perceptual data contribute to the imbalance trait in IoT-based systems. Because the calculation capabilities of IoT capture devices and sensors are

International Symposium on Smart Cities Challenges Technologies and Trends Technologies (SCCTT 2023), December 07–12, 2023, Delhi, India

awotunde.jb@unilorin.edu.ng (J.B. Awotunde); ranjit.panigrahi@gmail.com (R. Panigrahi); biswajit.Brahma@gmail.com (B. Brahma); akashkrbhoi@gmail.com (A.K. Bhoi)

0000-0002-1020-4432 (J.B. Awotunde); 0000-0001-6728-5977 (R. Panigrahi); 0000-0003-2759-3224 (A.K. Bhoi)

limited, any categorization for such data should be updated in on-the-fly response time. The IoT security issues are not hidden from any organization, and their importance has been taken seriously in various organizations [8]. In recent years, Artificial Intelligence (AI) has been used to professionally and accurately handling security in IoT-based systems. The AI techniques help fill the gaps of fighting against intruders that attack information in IoT-based systems for their gains, thus significantly increasing the stakeholders' trust in IoT systems. IoT-based devices and sensors operate in hostile environments, where physical layer fraud is a real possibility.

A distributed denial of service (DDoS) attack, which sends enormous amounts of data by consuming bandwidth access, is the most serious breach [9], [10]. Over a thousand botnets are causing havoc on legitimate websites such as Amazon, eBay, Netflix, and even government agencies. AI is a data-driven technique in which the first step is to grasp the data. Unique attack behaviours are represented by several types of data, such as host activities and network activity. Network traffic indicates network behaviour, whereas server logs describe host behaviour, and numerous types of attacks exist, each with its own setup. As a result, selecting appropriate data sources to detect various risks based on the threat's characteristics is crucial. The DoS attack has the ability of sending multiple packets within a shortest time, and this is one of their key characteristics, thus the flow data is suitable for identifying DoS attacks [11], [12].

A secret channel is ideal for session data detection since it contains a data-leaking transaction between two IP addresses. Hence, advancements in deep learning algorithms can aid in the detection of specific network patterns [13], [14]. Therefore, this study proposes a CNN model with PSO to optimize a flexible and secure architecture for safeguarding large-scale IoT networks. The model was greatly enhanced by adding a deep learning algorithm to identify emerging vulnerabilities to the IoT network to detect anomalies. This paper has the following contributions:

- To detect intruders in an IoT environment, the team developed an advanced Deep Learning model termed the hybrid CCN-KPCA[15] technique.
- The effectiveness of the system underwent evaluation using an IoT-based network dataset generated in 2020, presenting a significant challenge in establishing a strong framework.
- A thorough performance comparison was executed with a recent research study utilizing the same dataset, considering various performance metrics.

2. Related Works

With the exponential growth of IoT devices protecting critical resources and associated services is becoming a challenging task for the service providers [16]. Malware and related attacks are the most common threats in IoT networks. Hackers utilise a range of tactics to detect and control the behaviour of vulnerable resources, including the entire computing environment. Traditional cyber-threat approaches such as security protocols, cryptography [17], access controls were shown to be ineffectual and no longer appropriate for delivering effective critical infrastructure protection [8], [18]. Therefore, efforts has been given to design stat of the art Intrusion Detection Systems (IDS) in a variety of computing environments [19]–[25]. The IoT has become a vital part of today's data and information transmission machinery, necessitating global network security [26]. The traditional Machine Learning (ML) and Deep Learning (DL) models are critical in the development of an intelligent system in cybersecurity based on IoT. As a result of IoT devices, most businesses and organisations have undergone digital revolutions. However, this has generated new problems and vulnerabilities that can be exploited quickly once hackers become aware of them. Qaddoura et. al [27] proposed an IDS using multistage classification approach for IoT framework. During the training procedure, the network data has been oversampled with the use of Synthetic Minority Oversampling Technique and Support Vector Machine. The main technique of this method is the use of Single Hidden Layer Feed-Forward Neural Network (SLFN) for network detection. Multistage IDS has also been explored by Anthi et al [28]. The IDS consists of three layers a stage to classify the malicious and benign instances and the last layer designed to detect attack types. The layered approach successfully detects DoS and man in the middle attacks. In a similar node a two layers classification approach using Naïve Bayes and k-Nearest Neighbour has been used to keep track of User to Root (U2R) and Remote to Local (R2L) attacks [29]. Similarly, to choose the aspects of malicious attack behaviours, a feature selection strategy [30] was presented, and the system provided an appropriate means of defending enterprises from cybercrime. For the detection of botnet attack at the host and network levels, ML algorithms have been proved effective in the IoT-based environment [30]. Similarly, host level attacks are also detected marvellously using deep leaning models [31]. To detect intrusion and improve the prior model, reference [32] proposed an intelligent mechanism model based on a decision-making process; they constructed a recurrent neural network (RNN). Reference [32] used autoencoder for feature extraction to select revenant features before using CNN for classification the dataset for any possible attacks.

Recently, an intelligent IDS has been proposed for IoT based environment, where the detector is able to protect all the devices connected directly to its interface[33]. The Passban detector successfully detect SSH brute force, HTTP, port scanning and SYN flood attacks. To boost feature extraction across layers, a CNN was employed to identify infiltration [34], and feature fusion techniques were applied to acquire the whole attack characteristics. Reference [35] developed a solution to protect IoT in healthcare by managing traffic and brightening the environment. Security measures for IoT systems have also been devised, as mentioned in [36] and [37]. In a similar node, Ullah et al [38] proposed a new botnet based IoT dataset to test various flow based intrusion detection systems. The logistic regression on the new botnet dataset shows 96% detection accuracy on 20 attack features in the training model.

The reviewed works have shown that deep learning models can significantly improve the accuracy and efficiency of IDSs in an IoT-based environment, thus retaining a low false alarm rate. Hence, the study proposes a hybrid CNN-enabled PCA feature extraction and classification of anomaly trends detection in IoT-based systems. The PCA methods reduce the feature to minimize and useful one, thereby increasing the accuracy of the proposed model for detecting an intruder on an IoT-based system.

3. The Method

The approaches that are employed in accordance with the KPCA-CNN [15] framework consist of three primary stages: (i) preprocessing, (ii) feature selection, and (iii) classification. During the preprocessing phase, nominal qualities are initially transformed into numeric features in order to streamline later processing steps. The process of feature selection entails employing Kernel Principal Component Analysis (KPCA) to discover significant attributes within each class, hence lowering the dimensionality of the vector. The CNN model is utilized for the purpose of classifying events inside the IoTID20 dataset, with a specific focus on identifying potential attacks.

The data preparation stage primarily covers two main ways. First and foremost, the process of data conversion entails the translation of nominal properties into numerical features in order to facilitate subsequent processing. Additionally, the objective of data normalization is to address the significant variability of attributes by constraining values to a rational range. The normalizing process can be theoretically defined by equation (1) through the utilization of the minimum-maximum scaling method.

$$Y = \frac{Y - min(Y)}{max(Y) - min(Y)} \tag{1}$$

where dataset feature value is indicated by Y, and it is in the range of [0, 1].

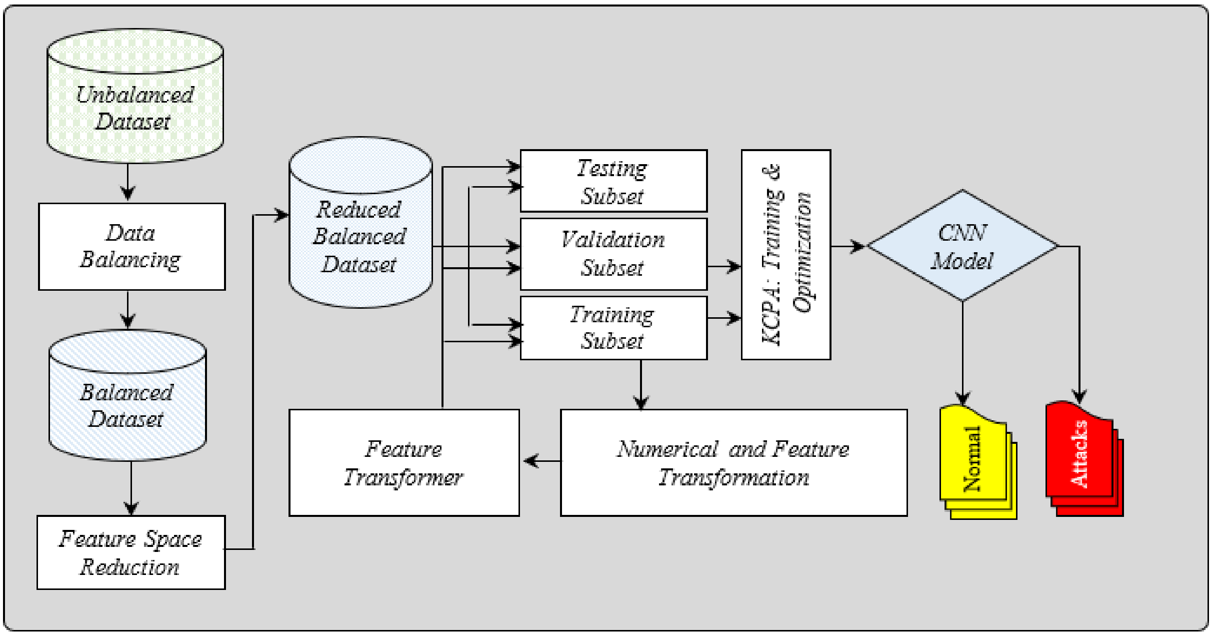

Figure 1: The CNN-KPCA IoT-based Intrusion Detection Framework

Before the data are exposed to feature extraction, they are put through preprocessing, during which PCA (Principal Component Analysis) is utilized the majority of the time to reduce the size of the dataset. However, due to the fact that PCA is unable to accommodate non-linear data features, particularly in complex structures, an alternate method such as KPCA is required in order to successfully overcome this constraint.

A convolution kernel is applied within the convolution layer in order to progress the learning and classification process. This results in the generation of a new feature graph that is comprised of numerous interconnected feature graphs. These interconnected feature graphs are utilized as an input signal for distinct convolution cores. Convolving many feature graphs together produces each output feature graph, which in turn contributes to the formation of another output layer [39]. The computation is carried out as follows within the convolution layer:

$$X_j^l = f\left(\sum_{i\epsilon M_j} X_i^{l-1} \mathrm{x} K_{ij}^l + b_j^l\right) \tag{2}$$

where X_j^l represents the j feature and the layer map l, K_{ij}^l represents the convolutional kernel function, f represents the activation function, and both b_j^l and M_j represents bias parameter and the input feature graph respectively.

4. The dataset

The newly developed IoTID20 attack dataset was generated in the year 2020 [40]. The dataset included 80 features from PCAP files, with two basic class label attacks and normal. Table 1 lists all of the IoTID20 dataset assaults, whereas Table 2 lists the number of characteristics for each class label.

Table 1
Varieties of Attacks in the IoTID20 Dataset

Scan	Mitm	Mirai	DOS
Host Port	ARP Spoofing Services	Brute Force (Host) Flooding (HTTP) Flooding (UDP)	Syn Flooding

Table 2
The number of attack occurrences in the IoTID20 dataset for each class

Class	Number of Instances
Attack Flooding (Mirai)	55124
UDP Flooding (Mirai)	183554
DoS	59391
HTTP Flooding (Mirai)	55818
Port DoS (Scan)	53073
Brute Force (Mirai)	121181
Host Port (Scan)	22192
MITM	35377
Normal	40073

5. Results and Discussion

The research employed actual data obtained from an Internet of Things (IoT) cybersecurity network. The CNN-KPCA model was utilized to categorize different types of threats present in the network dataset. The utilization of the KCPA model yielded notable enhancements in feature extraction, leading to substantial gains in both classification performance and model correctness. Significantly, the procedure of feature selection successfully decreased the total number of features from 81 to 19, identifying these specific features as the most essential components for detecting intrusions inside the dataset.

The dataset consisted of a total of 625,783 instances. To provide a comprehensive analysis, the data was divided into two partitions: 80 percent (500,627 instances) were allocated for training purposes, while the remaining 20 percent (125,155 instances) were reserved for testing. This division was necessary due to the large number of examples in the dataset. Table 3 presents a wide array of measures utilized to assess the performance of the suggested model.

Table 3
The number of attack occurrences in the IoTID20 dataset for each class

Models	Acc (%)	Sen (%)	Spe (%)	Pre (%)	F1-Score	Time (Sec)
CNN	97.49	99.32	91.05	98.52	98.73	79
CNN-KPCA	99.35	99.71	91.26	98.57	99.21	79

The suggested model produced the best outcomes when tested against the IoT-based dataset utilized for performance data from the network to detect infiltration. The overall effectiveness of the suggested CNN-KPCA model is shown in Figure 2. The IDS model performance is evaluated in Table 3 using two classes of attacks and the baseline condition; the CNN-KPCA model performs better, with 99.35% accuracy, 99.71% sensitivity, 91.26% specificity, 98.57 precision, and 99.21% F1-score, respectively.

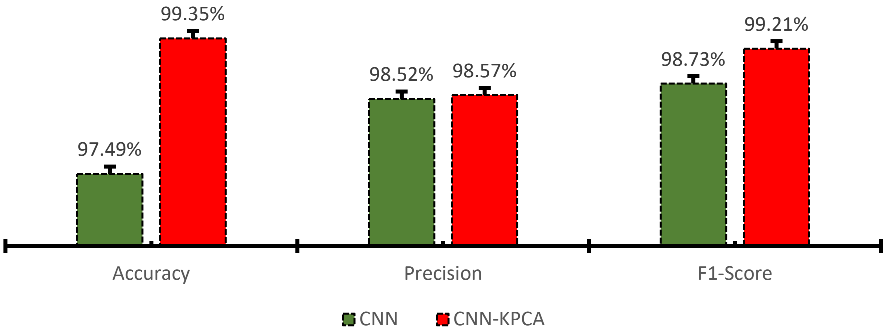

Figure 2: Performance evaluation of CNN-KPCA model

Recent research investigations that used the same dataset as the CNN-KPCA model were compared with it, particularly the research that produced the dataset used for evaluation. Several ML-based models, including Linear Discriminant Analysis (LDA), Decision with Random Forest, Support Vector Machine (SVM), and Gaussian Nave Bays (NB) from the IoT-based platform, were utilized in the baseline analysis on the dataset for the identification of intrusions [39]. Another important study by authors in [12] used CNN, LSTM, and CNN-LSTM on the same dataset and minimized the features from the network dataset from 81 to 21 revenant features using the particle swarm optimization approach (PSO). In order to further increase the accuracy of intrusion detection on the dataset, this study suggested CNN-KPCA. In order to handle the unbalanced data and minimize the number of characteristics from 81 to 19, the KCPA model was employed. This helped the suggested model accurately identify attackers on the IoT-based platform.

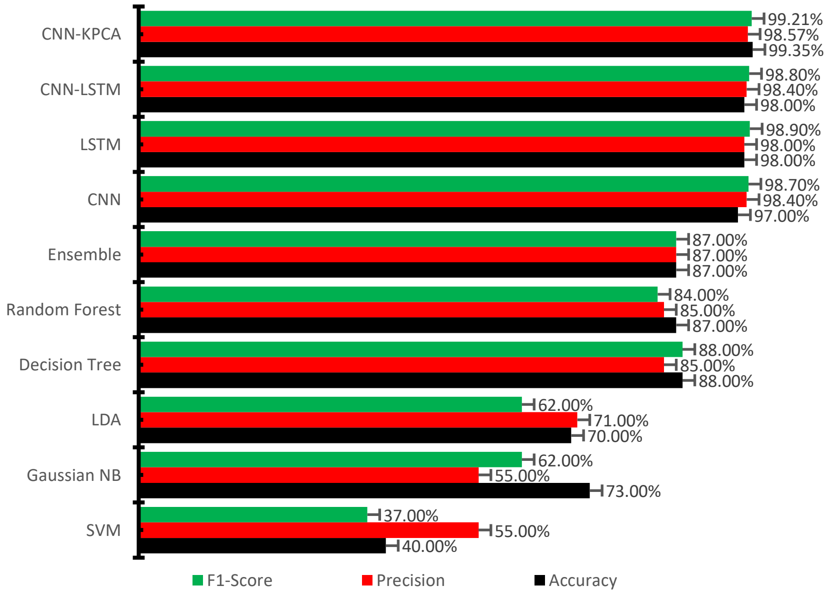

Figure 3: Comparison of the CNN-KPCA model and the existing models

From Figure 3, the results show that the CNN-KPCA framework performed better and yielded a better detection accuracy using various metrics with other ML models.

Table 4
Comparison of the CNN-KPCA model and the existing models

Models	Acc (%)	Sen (%)	Spe (%)	Pre (%)	F1-Score
SVM [40]	40.00	-	-	55.00	37.00
Gaussian NB [40]	73.00	-	-	55.00	62.00
LDA [40]	70.00	-	-	71.00	62.00
Decision Tree [40]	88.00	-	-	85.00	88.00

Random Forest [40]	87.00	-	-	85.00	84.00
Ensemble [40]	87.00	-	-	87.00	87.00
CNN [12]	97.00	99.01	77.20	98.40	98.70
LSTM [12]	98.00	99.67	71.60	98.00	98.90
CNN-LSTM [12]	98.00	99.23	77.40	98.40	98.80
CNN-KPCA	99.35	99.71	91.26	98.57	99.21

Table 4 presents a comprehensive comparison of various machine learning and deep learning models that have been implemented with the intention of achieving the particular goal of detecting intrusions in IoT environments. The models under discussion encompass a range of techniques, spanning from conventional machine learning approaches like SVM, Gaussian Naive Bayes (NB), LDA, Decision Trees, Random Forest, and Ensemble methods, to more intricate deep learning architectures such as CNN, Long Short-Term Memory (LSTM), CNN-LSTM, and the suggested CNN-KPCA hybrid model.

The traditional machine learning models displayed a level of performance that is commendable or at least respectable. An accuracy rate of 40% was demonstrated by the SVM technique. On the other hand, the accuracy reached by Decision Trees was the greatest at 88%. Having said that, it is important to highlight the fact that their accuracy and F1-scores were significantly lower than average. Based on this discovery, Decision Trees may have specific limitations when it comes to efficiently handling the complexities connected with intrusion detection in IoT systems. Despite this, the Gaussian NB, LDA, Random Forest, and Ensemble approaches all demonstrated equal levels of accuracy, with ratings ranging from around 70% to 87%. Although these models offer a satisfactory comprehension of the data, their capacity to identify complex patterns within the IoT data may be constrained. In contrast, deep learning models, specifically CNN, LSTM, and CNN-LSTM, have exhibited superior performance compared to standard models, achieving accuracies ranging from 97% to 98%. It has been proved that these models are successful in managing the complexities of IoT data and extracting sophisticated features for the purpose of conducting intrusion detection.

The CNN-KPCA model, which had outstanding performance, made use of a hybrid approach that synergistically merged the capabilities of CNN and KPCA. This allowed the model to more effectively analyze complex data. The model that was given shown outstanding performance, obtaining an accuracy rate of 99.35 percent, a precision value of 98.57%, and an incredible F1-Score of 99.21%. The CNN-KPCA model demonstrated a noteworthy specificity of 91.26%, indicating a strong capability to accurately detect non-intrusive occurrences in IoT data. The outstanding performance of this hybrid model suggests that it has the ability to effectively identify intrusions in IoT environments while producing only a limited number of false positives. As a consequence of this, it exhibits promise as an option that might potentially be used for the development of reliable intrusion detection systems in these complex environments.

In a nutshell, traditional machine learning methods have made important contributions toward a more fundamental understanding of intrusion detection. However, the application of more complex models, such as the hybrid model comprised of CNN and KPCA, has shown significant progress in performance enhancements. In the context of intrusion detection, this underlines how important it is to incorporate deep learning and hybrid approaches in order to successfully address the unique aspects of IoT data.

6. Conclusion

The proliferation of ransomware and malicious botnets in the realm of IoT systems poses a substantial risk to the privacy of users. These threats have the ability to intentionally focus on IoT systems in various industries, potentially resulting in significant harm that could affect the assets of several clients, particularly in vital domains such as healthcare, banking, smart cities, and others. The mitigation of these hazards requires the implementation of strong network intrusion detection systems (NIDSs) that are capable of efficiently detecting and mitigating online attacks. These systems play a crucial role in ensuring the security of networks. This study presents a novel approach that combines DL techniques to develop a model capable of detecting intrusions in networks based on the IoT. The research use the KPCA model as a means to identify key components that are vital for the detection of unauthorized individuals within IoT network platforms. Following this, a CNN is utilized to categorize the dataset based on the IoT, so assessing the effectiveness of the model proposed. The results of the performance evaluations demonstrate that the proposed model exhibits superior performance compared to currently employed approaches, with a remarkable accuracy rate of 99.35%. This demonstrates a significant improvement of 1.35% in accuracy when compared to the nearest CCN-LSTM models that utilized the identical dataset.

Future study should aim to investigate contemporary classification approaches and design concepts in order to evaluate the robustness of IDS against a wide range of threats. The exploitation of conventional deep learning methods by intruders frequently results in notable instances of false alarms. This emphasizes the necessity for adaptive strategies to effectively address these difficulties.

References

[1] M. Trziszka, "Internet of Things in the Enterprise as a Production Process Control System," in *International Conference on Applied Human Factors and Ergonomics*, 2020, pp. 56–62.

[2] A. A. A. Sen and M. Yamin, "Advantages of using fog in IoT applications," *Int. J. Inf. Technol.*, vol. 13, no. 3, pp. 829–837, 2021.

[3] C. Adams *et al.*, "Monarch: Google's planet-scale in-memory time series database," *Proc. VLDB Endow.*, vol. 13, no. 12, pp. 3181–3194, 2020.

[4] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and security concerns in IoT-based healthcare systems," in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*, Springer, 2021, pp. 105–134.

[5] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Futur. Gener. Comput. Syst.*, vol. 113, pp. 418–427, 2020.

[6] P. Dahiya and D. K. Srivastava, "Network intrusion detection in big dataset using spark," *Procedia Comput. Sci.*, vol. 132, pp. 253–262, 2018.

[7] J. B. Awotunde, A. K. Bhoi, and P. Barsocchi, "Hybrid Cloud/Fog Environment for Healthcare: An Exploratory Study, Opportunities, Challenges, and Future Prospects," in *Hybrid Artificial Intelligence and IoT in Healthcare*, Springer, 2021, pp. 1–20.

[8] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021.

[9] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput. Sci. Rev.*, vol. 39, p. 100332, 2021.

[10] U. Kumar, S. Navaneet, N. Kumar, and S. C. Pandey, "Isolation of ddos attack in iot: A new perspective," *Wirel. Pers. Commun.*, vol. 114, pp. 2493–2510, 2020.

[11] A. Dahiya and B. B. Gupta, "Multi attribute auction based incentivized solution against DDoS attacks," *Comput. \& Secur.*, vol. 92, p. 101763, 2020.

[12] H. Alkahtani and T. H. H. Aldhyani, "Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms," *Complexity*, vol. 2021, 2021.

[13] T. Aldhyani and M. R. Joshi, "Analysis of dimensionality reduction in intrusion detection," *Int. J. Comput. Intell. Informatics*, vol. 4, no. 3, pp. 199–206, 2014.

[14] S. Venkatraman and M. Alazab, "Use of data visualisation for zero-day malware detection," *Secur. Commun. Networks*, vol. 2018, 2018.

[15] J. B. Awotunde, T. Gaber, L. V. N. Prasad, S. O. Folorunso, and V. L. Lalitha, "Privacy and Security Enhancement of Smart Cities using Hybrid Deep Learning-enabled Blockchain," *Scalable Comput. Pract. Exp.*, vol. 24, no. 3, pp. 561–584, 2023.

[16] L. Edwards, "Privacy, security and data protection in smart cities: A critical EU law perspective," *Eur. Data Prot. L. Rev.*, vol. 2, p. 28, 2016.

[17] R. O. Ogundokun, J. B. Awotunde, E. A. Adeniyi, and F. E. Ayo, "Crypto-Stegno based model for securing medical information on IOMT platform," *Multimed. Tools Appl.*, pp. 1–23, 2021.

[18] F. E. Ayo, S. O. Folorunso, A. A. Abayomi-Alli, A. O. Adekunle, and J. B. Awotunde, "Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection," *Inf. Secur. J. A Glob. Perspect.*, vol. 29, no. 6, pp. 267–283, 2020.

[19] R. Panigrahi and S. Borah, "Dual-stage intrusion detection for class imbalance scenarios," *Comput. Fraud Secur.*, vol. 2019, no. 12, 2019, doi: 10.1016/S1361-3723(19)30128-9.

[20] T. Yu and X. Wang, "Topology Verification Enabled Intrusion Detection for In-Vehicle CAN-FD Networks," *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 227–230, 2020, doi: 10.1109/LCOMM.2019.2953722.

[21] J. Zhang, M. Zulkernine, and A. Haque, "Random-Forests-Based Network Intrusion Detection Systems," *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 38, no. 5, pp. 649–659, 2008, doi: 10.1109/TSMCC.2008.923876.

[22] R. Panigrahi *et al.*, "A Consolidated Decision Tree-Based Intrusion Detection System for Binary and Multiclass Imbalanced Datasets," *Mathematics*, vol. 9, no. 7, p. 751, Mar. 2021, doi: 10.3390/math9070751.

[23] H. Sadreazami, A. Mohammadi, A. Asif, and K. N. Plataniotis, "Distributed-Graph-Based Statistical Approach for Intrusion Detection in Cyber-Physical Systems," *IEEE Trans. Signal Inf. Process. over Networks*, vol. 4, no. 1, pp. 137–147, 2018, doi: 10.1109/TSIPN.2017.2749976.

[24] R. Panigrahi *et al.*, "Performance Assessment of supervised classifiers for designing intrusion detection systems: A comprehensive review and recommendations for future research," *Mathematics*, vol. 9, no. 6, p. 690, 2021.

[25] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," *IEEE Trans. Syst. Man, Cybern. Part B*, vol. 38, no. 2, pp. 577–583, 2008, doi: 10.1109/TSMCB.2007.914695.

[26] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, and T. Eschert, "Industrial internet of things and cyber manufacturing systems," in *Industrial internet of things*, Springer, 2017, pp. 3–19.

[27] R. Qaddoura, A. Al-Zoubi, I. Almomani, and H. Faris, "A Multi-Stage Classification Approach for IoT Intrusion Detection Based on Clustering with Oversampling," *Appl. Sci.*, vol. 11, no. 7, p. 3022, 2021.

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

[29] 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 Trans. Emerg. Top. Comput.*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.

[30] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Networks*, vol. 151, pp. 147–157, 2019.

[31] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 761–768, 2018.

[32] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 88–95, 2018.

[33] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.

[34] H. Yang and F. Wang, "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network," *IEEE Access*, vol. 7, pp. 64366–64374, 2019, doi: 10.1109/ACCESS.2019.2917299.

[35] S. S. Chakravarthi and S. Veluru, “A review on intrusion detection techniques and intrusion detection systems in MANETS,” in *2014 International Conference on Computational Intelligence and Communication Networks*, 2014, pp. 730–737.

[36] L. Santos, C. Rabadao, and R. Gonçalves, “Intrusion detection systems in Internet of Things: A literature review,” in *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 2018, pp. 1–7.

[37] G. Kanagaraj, S. G. Ponnambalam, and N. Jawahar, “Trends in intelligent robotics, automation, and manufacturing,” *Commun Comput Inf Sci*, vol. 330, pp. 491–501, 2012.

[38] I. Ullah and Q. H. Mahmoud, “A Technique for Generating a Botnet Dataset for Anomalous Activity Detection in IoT Networks,” in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2020, pp. 134–140.

[39] S. Lawrence, C. L. Giles, A. C. Tsoi, and A. D. Back, “Face recognition: A convolutional neural-network approach,” *IEEE Trans. neural networks*, vol. 8, no. 1, pp. 98–113, 1997.

[40] I. Ullah and Q. H. Mahmoud, “A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks.,” in *Canadian Conference on AI*, 2020, pp. 508–520.