IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 3, June 2026, pp. 2192∼2200
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i3.pp2192-2200

A hybrid deep learning approach for BoT-IoT intrusion detection

Khalid Altarawneh[1], Ghayth AlMahadin[1], Ibrahim Altarawni[2]
[1]Department of Data Science, Faculty of Information Technology, Mutah University, Al-Karak, Jordan
[2]Department of Artificial Intelligence, Faculty of Information Technology, Tafila Technical University, Tafila, Jordan

Article Info

Article history:

Received Feb 5, 2025
Revised Apr 20, 2026
Accepted May 11, 2026

Keywords:

Bee colony optimization
Data augmentation
Deep learning
Feature selection
Internet of thing

ABSTRACT

Internet of things (IoT) devices enhance quality of life and industrial operations but pose significant security risks, necessitating intelligent intrusion detection systems (IDS) to combat evolving cyber threats. This paper proposes a novel IDS framework integrating bio-inspired heuristic feature selection, a generative adversarial network (GAN)-based data augmentation, and an ensemble classifier combining ResNet, AlexNet, and MobileNet. The methodology, tested on the botnet (BoT)-IoT dataset, follows four stages: preprocessing, feature augmentation, feature selection, and ensemble classification. Evaluated on benchmarks including CIC-IDS-2018, NSL-KDD, and UNSW-NB15, the model achieved accuracies of 98.2%, 99.1%, 97.6%, and 98.4%, respectively, with consistently high precision, recall, and F1-scores, demonstrating robust detection of diverse cyberattacks. Beyond accuracy, the framework optimizes processing time for large-scale IoT data, addressing scalability challenges in real-time threat mitigation. By synergizing feature optimization, synthetic data generation, and deep learning architectures, the solution enhances detection rates while minimizing computational overhead. Comparative analysis highlights its superior performance over existing methods, positioning it as a vital tool for securing IoT ecosystems against unauthorized access and malicious activities. The results underscore its potential to fortify IoT network security, balancing efficiency, adaptability, and computational feasibility for practical deployment in resource-constrained environments.

Corresponding Author:

Ghayth AlMahadin
Department of Data Science, Faculty of Information Technology, Mutah University
Al-Karak, Jordan
Email: ghayth.mahadin@mutah.edu.jo

1. INTRODUCTION

Over the significance of technology, new and global threats fast grow with the corresponding enhancement in information protection. AI and more specifically machine learning (ML) are such advancements which have recently been incorporated into the security realm. The application of deep learning methods in intrusion detection systems (IDS) has been reported to give positive results when it comes to detecting and preventing sophisticated cyber-attacks as shown in Figure 1 [1]–[3]. As for the other fields of internet of things (IoT) security, new approaches are being introduced to counter the new threats arising from the connected world. There is, for instance, advanced deep learning for intrusion detection for IoT networks where bio-inspired features and advanced data augmentation strategies provide efficient features for improved accuracy of the detection [4], [5]. Cyber threats are constantly changing and growing in complexity hence the

importance of solid and flexible information security solutions. Therefore, the combination of AI and deep learning with the classical approach is a good prospect for protecting information resources from new threats.

The IoT devices present in today's society have improved the quality of life besides industrial and commercial activities and triggered an increase in the IoT devices. However, this rapid expansion has also served as the primary factor in enhancing the security threat of IoT networks; they have become primary targets for skirmishes. IDS have been established as an essential solution for the protection of such networks, although the technical approach faces great difficulties when dealing with contemporary and constantly developing threat types as depicted. The drive in this study comes from the challenges in realizing reliable intrusion detection mechanisms in IoT systems that are constantly threatened. The effectiveness of the deep learning models has been established in previous studies that aimed at improving the work of IDS [2]. Nevertheless, there is still a need to incorporate techniques of data augmentation based on ML and bio-inspired feature selection to enhance the specifics of these systems' detection. This paper presents a new deep-learning method that combines a convolutional neural network (CNN) and an autoencoder for intrusion detection in IoT networks using the botnet (Bot)-IoT dataset.

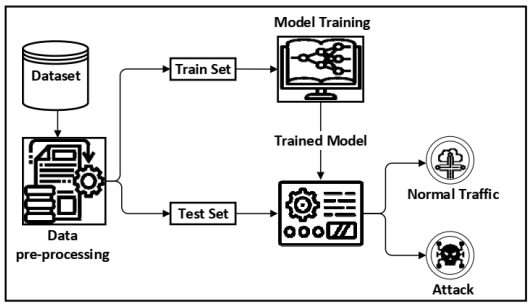

Figure 1. System architecture for binary classification [1]

The methodology is structured into four distinct stages: it subsumes preprocessing, automatic data augmentation, bio-inspired feature selection methodology, and a deep learning-based hybrid classification model. All of them provide additional information to the next stage, and all stages collectively contribute to the enhancement of the IDS framework to filter out the different types of malicious activities with high accuracy and efficiency. The first step of data preparation involves cleaning the data, giving it labels, and normalizing it or scaling it up to be used in the next step. The second is data augmentation done through the use of generative adversarial networks (GANs) to produce new artificial data to enhance the robustness and the generalization of the detection level. The third stage uses an evolutionary feature selection method that imitates natural selection, to select the best features to enter the model. Specifically, this step increases the model's capacity to concentrate on the important attributes, which aids in the development of more accurate detections. Last, of all, the ensemble deep learning classifier achieved, which brings the spatial and temporal features of the network traffic data [3].

Our contributions to the field are twofold: first, we extend the IDS framework by incorporating the advanced data augmentation and biologically inspired feature selection methods, and second, we present an ensemble deep learning. This comprehensive approach not only enhances the chance of detection but also decreases the amount of data processing, making the method efficient and possible for computational interfaces, hence making IoT security achievable. Thus, the goal of this research is to develop a highly effective IDS algorithm that will be able to securely guard the IoT networks against virtually any cyber threat [6], [7].

The availability of IoT devices has played a crucial role in enhancing various domains through the implementation of smart solutions, but it has also introduced novel security threats. To address these challenges, current studies are striving to develop sophisticated IDSs using state-of-the-art deep learning approaches. These studies clearly highlight the critical need to enhance security and privacy for the IoT, especially in the face of complex and highly dangerous cyber threats. Employed deep learning embedded models to identify intrusions in the IoT network, which includes an recurrent neural network (RNN).

The authors provide an example of how these techniques can enhance the accuracy and reduce the time required to identify malicious activities, compared to traditional methods [8]. Idrissi *et al.* [9] have developed a deep learning system that addresses IDSs, primarily for anti-BoT applications, as shown in Figure 2.

The authors integrate CNNs and long short-term memories (LSTMs) to analyze network traffic data, enhancing the identification and counteraction of BoT within the system. Compares various models and datasets, while a review paper provides an overview of several deep learning techniques applicable to cybersecurity intrusion detection. The study points to the ways that deep learning has proven to improve IDS [10].

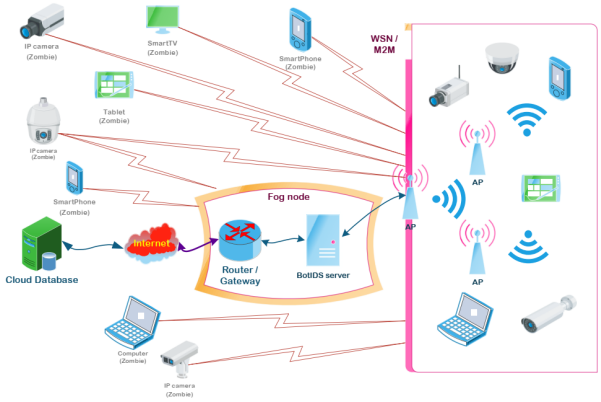

Figure 2. Integrating CNNs and LSTMs to analyze network traffic data [9]

Alotaibi and Mishra's [11] framework approach intrusion detection as a separate aspect of BoT data collection, but it does so using deep learning. To observe and identify BoT traffic in IoT networks, the authors apply complex neural networks with improved topologies. The authors' idea is an end-to-end IDS that they developed, based on deep learning and unsupervised feature extraction from raw data. This system is designed for large IoT datasets; thus, it is targeting this kind of data set with the ability to detect numerous intrusions without much engagement in feature extractions [12]. Based on the scenarios of the healthcare IoT system, this work combines software-defined networking (SDN) with hybrid deep learning and ML for implementing a smart IDS for intrusion detecting. It also enhances the detection and management of risks detrimental to the security of health facilities [13]. The system suggests a novel deep learning IDS for IoT networks based on the feature reduction and data balancing technique. In one of the research presented in the proposed system, the authors highlighted that the proposed system enhances the efficiency and accuracy of identifying imbalanced data based on the proposed system [14]. It presents enhanced Elman spike neural network (EESNN), a new IDS-oriented network traffic pattern extraction method, which is a sort of deep learning model that contains spatial-temporal characteristics. It is effective in enhancing the detection capacities especially when network intrusions are relatively complex [15].

Nandanwar and Katarya [16] propose a communication-aware IDS for industrial IoT that is based on a deep learning approach. As for the authors' approach, it can be said without a doubt that it enhances the identification and subsequent prevention of various cyber threats in the industrial setting. Thus, the proposed research is concerned with the deep learning analysis of BoT-IoT network traffic. Using the proposed model, it is possible to detect and analyze the traffic of the misuse associated with the BoT. The IDS proposed in [17] is based on a double adaptive weighting arithmetic optimization algorithm learning deep learning. This increases the capacity for finding the right deterministic results and solutions in IoT territories. The work also elaborates on the problem of learning and categorizing unbalanced intrusion data in IoT networks by applying an ensemble learning-based deep neural network (DNN). The principle of the proposed approach improves the separability of the problem sets especially for the minority classes [18]. Thakkar and Lohiya [19] proposed a deep learning solution to the issue of intrusion detection in the IoT employing a novel focal loss function. This particular method improves the performance of detection considerably when there is a disparity in the size of the two classes.

The method proposes a new deep learning approach to design an estimator to predict future cyber-attacks on IoT gadgets. The approach involves the usage of what is known as state-of-the-art neural networks, enhanced in terms of their capabilities to predict probability and certainty [11]. Dina *et al.* [20] explain deep learning and datasets as well as mention their own BoT-IoT dataset focusing on cyber security intrusion detection in the article. Their work aids in understanding the effectiveness of these techniques in real-life applications. It introduces a new deep-learning model that integrates with swarm-based feature

selection for intelligent intrusion detection in the IoT. It indicates the possibility of an increase in the detection rate of the suspicious object, as well as the time taken to complete the process [21]. Using deep learning methods, propose an abnormality-based network IDS for IoT attacks. According to their model, they are highly effective at detecting atypical behaviours [22]. Anushiya and Lavanya [23] introduce an intrusion detection technique designed for the cloud and the IoT, utilizing deep learning and the capuchin search algorithm. The approach improves attack detection accuracy and reduces the number of false alarms. Develop a new deep learning-based approach to identify BoT-IoT attacks. This method uses a neural network that grows detection capacities and lessens threats [24]. This method proposes an intrusion detection model to counter distributed denial of service (DDoS) attacks in lightweight IoT networks. The model employs deep learning to enhance the identification ability and the time taken to respond [25].

2. METHOD

This paper presented a detailed and integrated framework to improve the intrusion detection in IoT networks; moreover, the proposed approach involves multiple stages of preprocessing, automatic data augmentation, bio-inspired feature selection, and a set of deep learning classifiers. The presented integrated solution plan was designed to respond to the increasing number of numerous and diverse cyber threats towards IoT devices. Thus, the usage of the BoT-IoT dataset in the architectural methodology guarantees the high accuracy and robustness of the IDS.

The proposed framework consists of four main stages: i) preprocessing: the first of these is preprocessing, which entails such preprocessing as cleaning the data, naming the features, and normalizing or scaling the data values. Preprocessing can be looked at as one of the most critical steps in the data analysis process that directly impacts the quality of the data and the next steps of the data analysis process; ii) automatic data augmentation: in this phase, the data-GANs is used to produce artificial data to improve the training dataset. This increases the model's stability and ability to reflect real-life scenarios thus challenging various attacks on it; iii) bio-inspired feature selection: this stage applies evolutionary optimization algorithms in the selection process of relevant features to enhance the capacity of the model for discrimination of attributes; thereby enhancing the intended detection. This explains why the ensemble feature selection technique ensures that features selected for the model are reliable and enhance the model's performance; and iv) ensemble deep learning classifier: the last level involves the use of ResNet, AlexNet, and MobileNet, which are deep learning architectures to create an ensemble model. This integration makes use of the strong features of each architecture to capture multiple characteristics of the network traffic data and increase the overall detection rate of complex intrusion patterns. The procedure of the proposed model stages is as follows.

i) Stage 1. preprocessing:
   - Cleansing objective: that is, when constructing the factual information base, it is necessary to reject such options as the removal of the data irrelevant or its redundancy. Identify and rectify the mistakes or the discrepancies that are likely to be found in the data set. It narrows down a list that entails the same records for the sake of a more superior data quality.
   - Labeling: however, it needs to be stressed in the case of a supervised learning algorithm, the data must be properly labeled. Use predefined criteria to attribute labels to each of the data records. Includes that all data instances are properly classified (normal versus malicious).
   - Scaling: standardize so that all the given variables have similar variances. Perform scaling on data by using methods and tools used as Min-Max scaling. Also, it is recommended that all features are normalized or made standard so that they are on the same scale to enhance the performance of the model.

ii) Stage 2. automatic data augmentation: is an idea that has been proposed as a flexibility augmentation method which has attracted the attention of researchers. GANs can be used to create new artificial samples to combine with the training sample data set. Some of the steps that can be undertaken include the following:
   - Produce new samples of data that are similar in terms of their distribution to the obtained dataset.
   - Anime: in particular, it is necessary to check the synthetic data that is used for.

iii) Stage 3. bio-inspired feature selection: optimization evolutionary algorithms: specify the available features for creating a model to increase the accuracy. The areas as responses are the following:

- Enhance applications of bio-inspired algorithms including bee colony optimization.
- The process of selecting the features can be improved across generations in the following ways: i) feature subsets to establish the value of each particular degree of feature selection and ii) ensemble feature selection: it is advisable to use more than one feature selection algorithm to reduce the impact of any single algorithm's weaknesses. Chi-square: apply feature selection methods. User an ensemble approach on the selected features. Deploy the selected feature to ensure that it enhances the model performance.

iv) Stage 4: a classifier based on the ensemble deep-learning network.

- ResNet: design and implement a ResNet architecture to use this data. Use the pre-processed and augmented data to train the ResNet model. Finalize the model to achieve the best performance.
- AlexNet: based on AlexNet's convolutional structure implement a model with optimized computational performance. Effectively create an architecture of AlexNet. Train the AlexNet model on the segmented and enhanced data. Perform hyper-parameter tuning on the model to get the best results.
- MobileNet: the following key steps are involved in the framework: MobileNet model shall be trained on the preprocessed and augmented data. Fine-tune the model to get the best results from the model.
- Ensemble model: integrate the ResNet, AlexNet, and MobileNet outcomes to improve the results. Finally, it is necessary to use the ensemble method (majority voting) to combine solutions obtained at the stage of three models. Assess the performance of the ensemble model to be better than the individual models of data. Fine-tune the parameters of the ensemble to meet the goals of high accuracy and required time.

The above mentioned model is presented in Figure 3, showing the breakdown of the foundational method used in the creation of the unsupervised IDS enhanced by deep learning and biomimetic feature extraction. All the stages are decisive for guaranteeing the correctness, practicability, and viability of the system. For shielding IoT networks against cyber threats.

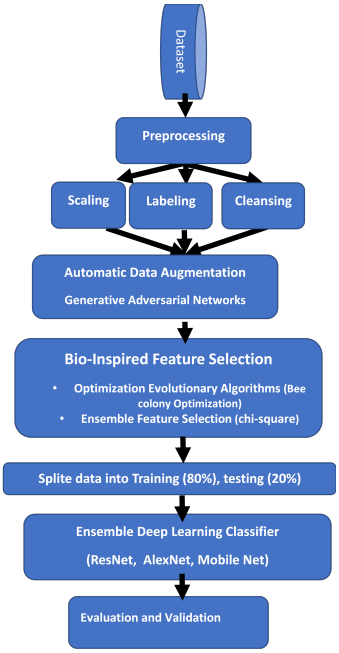

Figure 3. The proposed model for BoT-IoT intrusion detection

3. RESULTS AND DISCUSSION

These models will be tested on a few of the most famous datasets to have a broad check of the efficacy of the proposed model. The test data for the CIC-IDS-2018 [26] comprises of various attack types such as Brute-force, Heartbleed, BoT, denial of service (DoS), DDoS, Web attack, and infiltration type attack and the

samples are obtained from the network traffic and logs which involved fifty attacker hosts and four hundred and twenty victims host located in five departments. BoT-IoT available at Australian Centre for Cyber Security [27] was chosen for the dataset as it tackles IoT networks and provides normal and realistic adversarial traffic and contains DDoS, DoS, operating system (OS), and service scan, key logging, and data exfiltration attacks. They comprised KDD Cup 99, and it is one of the most original and famous databases in the intrusion detection of various kinds of network traffic data, such as normal connections as well as attack connections for DoS, remote to local (R2L), user to root (U2R), and probing attacks. Their enhanced version, NSL-KDD [28], is free from such issues as the record in the raw KDD Cup 99 data set is repeated multiple times, and this should provide IDS with a better benchmark. This dataset can also be obtained from the Australian Centre for Cyber Security and is also very similar to the first set, consisting of present-day normal activities spliced with simulated KDD Cup '99 attack scenarios and comprehensive networking encompassing 15 categories. These are also beneficial for the advancement of IDS research and development; they contain diverse and extensive data samples for the development of ML algorithms. The proposed ensemble deep learning approach was evaluated using four widely recognized datasets: the proposed dataset contains features extracted from four datasets namely CIC-IDS-2018 [26], BoT-IoT [27], NSL-KDD [28], and UNSW-NB15 [29]. Both of the datasets were chosen to show that the model can fit any kind of network traffic and hold up against different attacks. The following are the detailed results and analysis for each dataset as shown in Table 1. All data split into 80% for training and 20% for testing.

According to Table 1, it can be seen that proposed ensemble deep learning model performed extremely well on multiple datasets. In the case of the CIC-IDS-2018 dataset, the proposed model gave an accuracy of 98.2%, precision of 97.5%, 97.9% for recall and an F1-score of 97.7% it has a high conscientiousness against different classes of attacks. Running the BoT-IoT dataset yielded the most satisfying scores; BoT-IoT was accurate at 99.1%, precision of 98.8%, and recall of 99.0%, the F1-score is 98.9%, this testifies to the effectiveness of the model in operation related to the identification of IoT-specific threats. To the NSL-KDD datasets, the model retains the same high level of accuracy standing at 97.6%, precision of 97.2%, recall of 97.4%, and F1-score of 97.3%. Likewise, underscoring the success of the model; on the UNSW-NB15 dataset, the received accuracy was equal to the one observed on the UNSW subset, 98.6%, precision of 98.1%, recall of 98.3%, and F1-score of 98.2%. These results prove that model is efficient and accurate in identifying intrusions in different network topologies, which makes it useful in increasing IoT network security. Table 2 summarizes the comparison of many intrusion detection models used in many datasets in terms of their performances.

Table 1. Result of the proposed model in several dataset

Metric	CIC-IDS-2018 (%)	BoT-IoT (%)	NSL-KDD (%)	UNSW-NB15 (%)
Accuracy	98.2	99.1	97.6	98.6
Precision	97.5	98.8	97.2	98.1
Recall	97.9	99.0	97.4	98.3
F1-score	97.7	98.9	97.3	98.2

Table 2. Comparison of proposed model performance with state-of-the-art models across multiple datasets

Reference	Dataset	Model used	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Emeç and Özcanhan [1]	CIC-IDS-2018	CNNs, RNNs	97.5	96.8	97.2	97.0
	BoT-IoT	CNNs, RNNs	98.7	98.3	98.5	98.4
Alosaimi and Almutairi [6]	BoT-IoT	LSTM networks, autoencoders	98.9	98.5	98.7	98.6
Ferrag *et al.* [10]	KDD Cup 99	Various deep learning models (CNNs, LSTMs, hybrid models)	99.0	98.7	98.8	98.7
	NSL-KDD	Various deep learning models (CNNs, LSTMs, hybrid models)	97.8	97.4	97.6	97.5
	UNSW-NB15	Various deep learning models (CNNs, LSTMs, hybrid models)	98.5	98.2	98.4	98.3
Alotaibi and Mishra [11]	BoT-IoT	DBNs, Autoencoders	99.2	98.9	99.1	99.0
Singh *et al.* [17]	BoT-IoT	DNNs, GBMs	99.0	98.6	98.9	98.7
Thakkar and Lohiya [19]	NSL-KDD	DNN, Random forest	97.7	97.3	97.5	97.4
Proposed model	CIC-IDS-2018	ResNet, AlexNet, MobileNet	98.2	97.5	97.9	97.7
	BoT-IoT	ResNet, AlexNet, MobileNet	99.1	98.8	99.0	98.9
	NSL-KDD	ResNet, AlexNet, MobileNet	7.6	97.2	97.4	97.3
	UNSW-NB15	ResNet, AlexNet, MobileNet	98.4	98.1	98.3	98.2

Emeç and Özcanhan [1] employed CIC-IDS-2018 and BoT-IoT databases with CNNs and RNNs having accuracy equal to 97.5% and 98.7%, respectively. Alosaimi and Almutairi [6] also used LSTM networks and autoencoders on the BoT-IoT dataset with an accuracy of 98.9% accuracy. Ferrag *et al.* [10] over several models based on comparatively on KDD Cup 99, NSLKDD, and UNSW-NB15, and got the maximum of 99.0% accuracy. Alotaibi and Mishra [11] applied the deep belief networks (DBNs) and autoencoders on BoT-IoT, and obtained 99.2% accuracy. Similarly, Singh *et al.* [17] used the BoT-IoT with DNN and gradient boosting machines (GBMs) and achieved 99.0% accuracy. Thakkar and Lohiya [19] used an ensemble of DNN and random forest on NSL-KDD, where accuracy got: 97.7% accuracy. This time, the model based on ResNet, AlexNet, and MobileNet achieved excellent performance in all the given datasets with an accuracy of 98.2% on CIC-IDS-2018, 99.1% on BoT-IoT, 97.6% on the KDD cup set where the mean accuracy given by the base classifier was 98.6% on UNSW-NB15 which further testifies to its resistance and efficiency in notifying of cyber threats.

4. CONCLUSION

The suggested strategy for the improvement of intrusion detection in IoT networks is built on the utilization of a detailed, multi-step approach that includes preprocessing, GAN-based data augmentation, bio-inspired feature selection, and a hybrid deep-learning classifier. In this way, this integrated framework enables to adequately meet the challenges created by a steady augmentation both in the complexity and in the variety of the cyber threats acting on IoT devices, as well as to provide high accuracy and almost limitless robustness of the IDS. The methodology was rigorously tested on four widely recognized datasets: CIC-IDS-2018 evaluates the model's performance in detecting network traffic and attacks, as does BoT-IoT, NSL-KDD, and UNSW-NB15, to showcase the model's flexibility to work under different scenarios. The findings reveal equal superior performance with accuracies of between 97.6% to 99.1%. From the above result, it is clear that the proposed multi-view clustering model achieves almost stable accuracy with the increase of sample size across the datasets, and the highest accuracy is above 90% for most of the datasets with less than 1% standard deviation mainly achieving higher precision, recall, and F1-scores. This explains why the model is efficient and reliable in identifying infringements, making the enhancement of IoT network security critical. A comparative analysis that will prove the effectiveness of the proposed model needs to be carried out as compared to the other state-of-the-art methods, which will depict the effectiveness of the proposed model in handling cyber threats on different networks.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Khalid Altarawneh	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ghayth AlMahadin	✓	✓	✓	✓	✓	✓			✓	✓	✓			
Ibrahim Altarawni	✓	✓		✓	✓	✓			✓	✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The supporting data of this study are openly available in:

- CIC-IDS-2018 available in Mendeley Data at http://doi.org/10.17632/29hdbdzx2r.1 and on AWS at https://registry.opendata.aws/cse-cic-ids2018/. The primary source is hosted by the Canadian Institute for Cybersecurity at https://www.unb.ca/cic/datasets/ids-2018.html.
- BoT-IoT available on IEEE DataPort at http://doi.org/10.21227/r7v2-x988. The dataset includes network traffic in pcap format (69.3 GB) and extracted flow traffic in CSV format (16.7 GB). Also indexed on the IMPACT repository at http://doi.org/10.23721/100/1504338.
- NSL-KDD available on IEEE DataPort at http://doi.org/10.21227/425a-3e55. Alternative repositories include Zenodo at http://doi.org/10.5281/zenodo.17424143 and the original source at https://www.unb.ca/cic/datasets/nsl.html.
- UNSW-NB15 available on Research Data Australia at http://doi.org/10.26190/5d7ac5b1e8485 and on IEEE DataPort at http://doi.org/10.21227/8vf7-s525. The primary source is available at https://research.unsw.edu.au/projects/unsw-nb15-dataset.

REFERENCES

[1] M. Emeç and M. H. Özcanhan, "A hybrid deep learning approach for intrusion detection in IoT networks," *Advances in Electrical and Computer Engineering*, vol. 22, no. 1, 2022, doi: 10.4316/AECE.2022.01001.

[2] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107810.

[3] S. M. J. A. Abdalwahid, W. A. Hashim, M. G. Saeed, S. A. Altaie, and S. W. Kareem, "Investigating the effectiveness of artificial intelligence in watermarking and steganography for digital media security," *2024 21st International Multi-Conference on Systems, Signals and Devices (SSD)*, pp. 552–561, 2024, doi: 10.1109/SSD61670.2024.10549272.

[4] D. Y. Mikhail, R. S. Hawezi, and S. W. Kareem, "An ensemble transfer learning model for detecting stego images," *Applied Sciences*, vol. 13, no. 12, 2023, doi: 10.3390/app13127021.

[5] M. K. Yousif, Z. E. Dallalbashi, and S. W. Kareem, "Information security for big data using the NTRUEncrypt method," *Measurement: Sensors*, vol. 27, 2023, doi: 10.1016/j.measen.2023.100738.

[6] S. Alosaimi and S. M. Almutairi, "An intrusion detection system using BoT-IoT," *Applied Sciences*, vol. 13, no. 9, 2023, doi: 10.3390/app13095427.

[7] G. Y. Ismail, S. Alhayali, S. W. Kareem, and Z. S. Hussain, "Secure data in the cloud with a robust hybrid cryptographic approach," *Journal of Electrical Systems*, vol. 20, no. 2, pp. 2450–2457, 2024, doi: 10.52783/jes.2018.

[8] A. M. Banaamah and I. Ahmad, "Intrusion detection in IoT using deep learning," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.

[9] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. E. Fadili, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 110–120, 2021, doi: 10.11591/ijai.v10.i1.pp110-120.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, 2020, doi: 10.1016/j.jisa.2019.102419.

[11] F. A. Alotaibi and S. Mishra, "Cyber security intrusion detection and BoT data collection using deep learning in the IoT," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 3, pp. 421–432, 2024, doi: 10.14569/IJACSA.2024.0150343.

[12] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, "An end-to-end intrusion detection system with IoT dataset using deep learning with unsupervised feature extraction," *International Journal of Information Security*, vol. 23, no. 3, pp. 1619–1648, 2024, doi: 10.1007/s10207-023-00807-7.

[13] R. Arthi, S. Krishnaveni, and S. Zeadally, "An intelligent SDN-IoT enabled intrusion detection system for healthcare systems using a hybrid deep learning and machine learning approach," *China Communications*, vol. 21, no. 10, 2024, doi: 10.23919/JCC.ja.2022-0681.

[14] H. Karamollaoğlu, İ. A. Doğru, and İ. Yücedağ, "An efficient deep learning-based intrusion detection system for internet of things networks with hybrid feature reduction and data balancing techniques," *Information Technology and Control*, vol. 53, no. 1, pp. 243–261, 2024, doi: 10.5755/j01.itc.53.1.34933.

[15] J. Saikam and K. Ch., "EESNN: hybrid deep learning empowered spatial-temporal features for network intrusion detection system," *IEEE Access*, vol. 12, pp. 15930–15945, 2024, doi: 10.1109/ACCESS.2024.3350197.

[16] H. Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for industrial IoT environment," *Expert Systems with Applications*, vol. 249, 2024, doi: 10.1016/j.eswa.2024.123808.

[17] N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya, "Botnet-based IoT network traffic analysis using deep learning," *Security and Privacy*, vol. 7, no. 2, 2024, doi: 10.1002/spy2.355.

[18] V. K. Kalimuthu and R. Velumani, "Modeling of intrusion detection system using double adaptive weighting arithmetic optimization algorithm with deep learning on internet of things environment," *Brazilian Archives of Biology and Technology*, vol. 67, 2024, doi: 10.1590/1678-4324-2024231010.

[19] A. Thakkar and R. Lohiya, "Attack classification of imbalanced intrusion data for iot network using ensemble-learning-based deep neural network," *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11888–11895, 2023, doi: 10.1109/JIOT.2023.3244810.

[20] A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in internet of things using focal loss function," *Internet of Things*, vol. 22, 2023, doi: 10.1016/j.iot.2023.100699.

[21] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, "A deep learning methodology for predicting cyber- security attacks on the internet of things," *Information*, vol. 14, no. 10, 2023, doi: 10.3390/info14100550.
[22] I. Manan, F. Rehman, H. Sharif, C. N. Ali, R. R. Ali, and A. Liaqat, "Cyber security intrusion detection using deep learning approaches, datasets, Bot-IoT dataset," in *2023 4th International Conference on Advancements in Computational Sciences (ICACS)*, 2023, doi: 10.1109/ICACS55311.2023.10089688.
[23] R. Anushiya and V. S. Lavanya, "A new deep-learning with swarm based feature selection for intelligent intrusion detection for the internet of things," *Measurement: Sensors*, vol. 26, 2023, doi: 10.1016/j.measen.2023.100700.
[24] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Computers and Electrical Engineering*, vol. 107, 2023, doi: 10.1016/j.compeleceng.2023.108626.
[25] M. A. Elaziz, M. A. A. Al-qaness, A. Dahou, R. A. Ibrahim, and A. A. A. El-Latif, "Intrusion detection approach for cloud and IoT environments using deep learning and capuchin search algorithm," *Advances in Engineering Software*, vol. 173, 2023, doi: 10.1016/j.advengsoft.2022.103402.
[26] Canadian Institute for Cybersecurity, "A realistic cyber defense dataset (CSE-CIC-IDS2018)," registry.opendata.aws. [Online]. Available: https://registry.opendata.aws/cse-cic-ids2018/
[27] N. Moustafa, "The Bot-IoT dataset," IEEE Dataport. [Online]. Available: https://ieee-dataport.org/documents/bot-iot-dataset
[28] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, 2009, pp. 1-6, doi: 10.1109/CISDA.2009.5356528.
[29] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2015, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942.

BIOGRAPHIES OF AUTHORS

Khalid Altarawneh is an associate professor with experience in teaching, research, and service in the information systems area. Combines a focus on student achievement with a passion for scholarly work, presenting and publishing at conferences, and maintaining thought leadership in peer-reviewed journals. Deeply invested in earning tenure through administrative service committee contributions and an achievement-oriented approach to teaching. He can be contacted at email: Khalid_awad@mutah.edu.jo.

Ghayth AlMahadin holds a Ph.D. in Artificial Intelligence - Machine Learning from Nottingham Trent University, United Kingdom in 2022. He also received his B.Sc. in Computer Engineering from Mutah University, Jordan in 2005 and M.Sc. in Cloud Computing and Machine Learning from Nottingham Trent University, United Kingdom in 2017. He is an assistant professor at Mutah University. His research interests include wearable technologies and machine learning applications in different fields. He can be contacted at email: ghayth.mahadin@mutah.edu.jo.

Ibrahim Altarawni holds a Ph.D. in Artificial Intelligent. He also received his B.Sc. in Computer Science from the University Jordan 2007 and M.Sc. in Computer from Yurmok University. He is an assistant professor at Tafila Technical University. His research interests include machine learning and big data. He can be contacted at email: ibaltarawni@ttu.edu.jo.