IRAQI Academic Scientific Journals
Samarra Journal of Pure and Applied Science
SJPAS
www.sjpas.com
p ISSN: 2663-7405
e ISSN: 2789-6838

An Intelligent Intrusion Detection System Using Deep Learning and Multi-modal Fusion with RF Classification

Nuha Faris Abd El-Majeed [1*], Maytham Mustafa Hammood[2]
1- Department of Computer Science, Computer Science and Mathematics College, Tikrit University, Tikrit, Iraq

86https://doi.org/10.54153/sjpas.2026.v8i1.1286

Article Information
Received: 03/06/2025
Revised: 18/07/2025
Accepted: 16/08/2025
Published: 10/04/2026

Keywords:
IDS, CNN, DL, ML, Multimodal, RF.

Corresponding Author

E-mail: Nuha.F.abdEl-majeed4238@st.tu.edu.iq
Mobile: 07705142324

Abstract

The urgent demand for effective and intelligent intrusion detection systems (IDSs) to address this problem has grown in tandem with the increasing complexity and diversity of cyberattacks. With deep learning (DL) methods, the presented study aims to build an integrated framework that raises the intrusion detection accuracy and generalizability across several data sources. In this work, three well-known datasets, UNSW-NB15, NSL-KDD, and CICIDS2017, have been utilized. The suggested approach uses convolutional neural networks (CNNs) to extract deep features from such datasets. Dimensionality is reduced and irrelevant features are eliminated using principal component analysis (PCA). Combining the three datasets using a multimodal deep autoencoder (MDAE) extracts a new dataset. Final classification utilizes random forest (RF) technology, efficiently and precisely classifying network traffic using combined data. Supported by high precision, F1 score, and recall of 99.9%, evaluation findings show an excellent accuracy of the model of 99.9%. These results show how well modern classification algorithms, feature extraction, and multi-modal data fusion methods can be combined to create a sophisticated intrusion detection model capable of efficiently and consistently defending against challenging attacks.

Introduction:

Rising diversity and complexity of cyberattacks have made IDS more critical than ever [1]. These technologies are indispensable for protecting networks and private data from threats such as unauthorized access attempts, data leakage, and other malicious activities [2]. The three primary types of IDS are anomaly-based systems (AIDS), signature-based systems (SIDS) [3], and hybrid systems (HIDS). Their deployment location in network-based systems (NIDS) [4], and host-based systems (HIDS) allows for another division as well [5]. Particularly, machine learning (ML) [6] approaches and artificial intelligence (AI) have evolved into powerful tools for improving IDS performance and accelerating digital transformation [7]. These systems' capacity to dynamically detect anomalies in network traffic [8] helps them to adapt to new threats. In the case of dealing with multidimensional data [9], on the other hand, creating such systems presents significant difficulties that call for more advanced methods, such as DL. DL, especially CNNs [10], which are extraordinarily adept at detecting complex patterns in unstructured data [11], helps IDSs achieve

greater success. Moreover, such models enable automatic attack detection by eliminating the need for conventional feature engineering techniques, thereby enhancing system accuracy and reducing the necessity of expert intervention [12].

Moreover, they are ideal for assessing real-time data streams, thereby enhancing the capacity of security systems [13] to react quickly to new threats [14]. This work presents a comprehensive intrusion detection model that combines multi-source feature fusion using an MDAE with CNN feature extraction. The suggested approach uses dimensionality reduction and feature selection techniques, including PCA, to raise data quality and lower noise. An RF classification method was applied because of its high-accuracy classification abilities and efficiency in handling complex data. Three often utilized datasets, UNSW-NB15, NSL-KDD, and CICIDS2017, have been used to validate the suggested model's efficacy. The findings showed great accuracy and promising possibilities to raise ID performance in dynamic environments.

Related works:

DL-based IDSs have proliferated recently to handle increasingly complex cyber threats [15]. MDAEs and long short-term memory (LSTM) networks are combined in a sequential, multimodal intrusion detection model suggested here. On the NSL-KDD, UNSW-NB15, and CICIDS2017 datasets, our work attained 96% and 88% accuracy in multi-class and bi-class classification tasks, respectively [16]. In another study [17], using the KDD'99 dataset, a CNN was employed to identify malicious network traffic, achieving an accuracy and sensitivity of 97% and 93%, respectively. However, due to low specificity (25%), the model exhibited a high false positive rate, and its use of an outdated dataset limited its ability to detect complex attacks. In [18], a CNN-based intrusion detection system (IDS) was developed by introducing innovative preprocessing techniques for heterogeneous environments such as the Internet of Things and industrial control systems. Field-to-pixel encryption enabled learning of convolutional features directly from protocol-specific metadata. Although effective on the NSL-KDD dataset, the reliance on protocol knowledge reduced its generalizability across diverse networks. In [19], the model addressed class imbalance by converting one-dimensional vectors to two-dimensional images, enabling improved feature correlation across CNNs. The model was tested on NSL-KDD and CSE-CIC-IDS2018, achieving competitive results; however, it suffered from increased computational demand, making immediate deployment difficult. Similarly, in [2], a unified OCNN-HMLSTM model was proposed, combining optimized CNNs for spatial feature extraction and hierarchical LSTMs for temporal modelling. The model achieved an accuracy of over 90% on the NSL-KDD, IsSCX-IDS, and UNSW-NB15 datasets. However, high complexity and long training times were noted as drawbacks. In IoT environments [20], a few-shot CNN-IDS vulnerability detection system targeting zero-day threats was developed. The model was trained on UNSW-NB15 and Bot-IoT, achieving improved detection rates of 3–8%. However, its generalizability to large-scale or imbalanced datasets remained limited. In [21], a DCNN-based vulnerability detection system for IoT was proposed, utilizing feature engineering on NSL-KDD and incorporating cloud-aware loss functions to enhance performance. While strong results were achieved, balancing privacy and computational efficiency proved to be a significant challenge. In [22], an attention-based CNN was introduced to prioritize feature importance over 2D image representations, achieving fast and accurate detection on the CSE-CIC-IDS2018 dataset. However, the computational cost limited its deployment in constrained environments. In [23], CNNs and MLPs were utilized with feature selection via XGBoost and Pearson correlation, achieving 94% accuracy on the CIC-IDS2017 dataset. Although the simplification process was effective, it slightly reduced accuracy due to the loss of features. In [24], DCNNs trained on the ISCX-IDS 2012,

CICIDS2017/2018, and Kaggle DDoS datasets were utilized, achieving an accuracy of up to 100%. However, performance deteriorated in highly imbalanced scenarios, leading to rare attack types being missed. In [25], an ANN was designed using the NSL-KDD dataset with a custom architecture via Keras, achieving 97.5% accuracy and outperforming multiple baseline models. However, reliance on a single dataset limited the model's real-world applicability. In [26], SHM was presented, a hybrid anomaly detection framework that leverages 1D and 2D CNNs to analyze sensor signals. Despite its 95.1% accuracy, limited robustness to distributional transformations and anomaly generalization were observed. In [27], web threat detection focused on integrating semantic features from URL data using CNNs. The model achieved 99.16% accuracy across three datasets, although domain-specific feature mapping hindered generalizability. In [28], real-time cloud intrusion detection was addressed using CNNs and Random Forest (RF) feature selection on the CSE-CIC-IDS2018, achieving high accuracy and an F1 score of 97.52%. However, the high computational cost limits its applicability in resource-limited environments. In a later study [29], RF was applied to reduce the features of the UNSW-NB15 dataset before feeding it into a CNN, achieving an accuracy of 99.00%. However, the careful selection of features may have affected the detection of new threats, and using a single dataset limited generalizability.

Combining DL and ML approaches into a complete framework, the presented study attempts to create a multimodal prediction model to enhance the performance regarding IDSs. Three benchmark datasets, UNSW-NB15, NSL-KDD, and CICIDS2017, form the basis for the suggested model. The technique begins with preprocessing tasks, including normalization and encoding, and then utilizes CNNs for feature extraction. Following an MDAE, the three datasets are merged to produce a new dataset. PCA can be defined as a dimensionality reduction and feature selection method utilized to lower complexity and raise classification efficacy. The RF model is applied due to its outstanding classification performance and ability to handle complex data. The aim is to offer a consistent and efficient threat detection methodology for many types of network environments. Model performance is assessed using recall, F1 score, and precision measures.

Methodology:

This work aims to enhance the efficiency of IDS through advanced approaches, including dimensionality reduction, feature extraction, and classification improvement. Figure 1 illustrates the overall framework of the proposed technique steps.

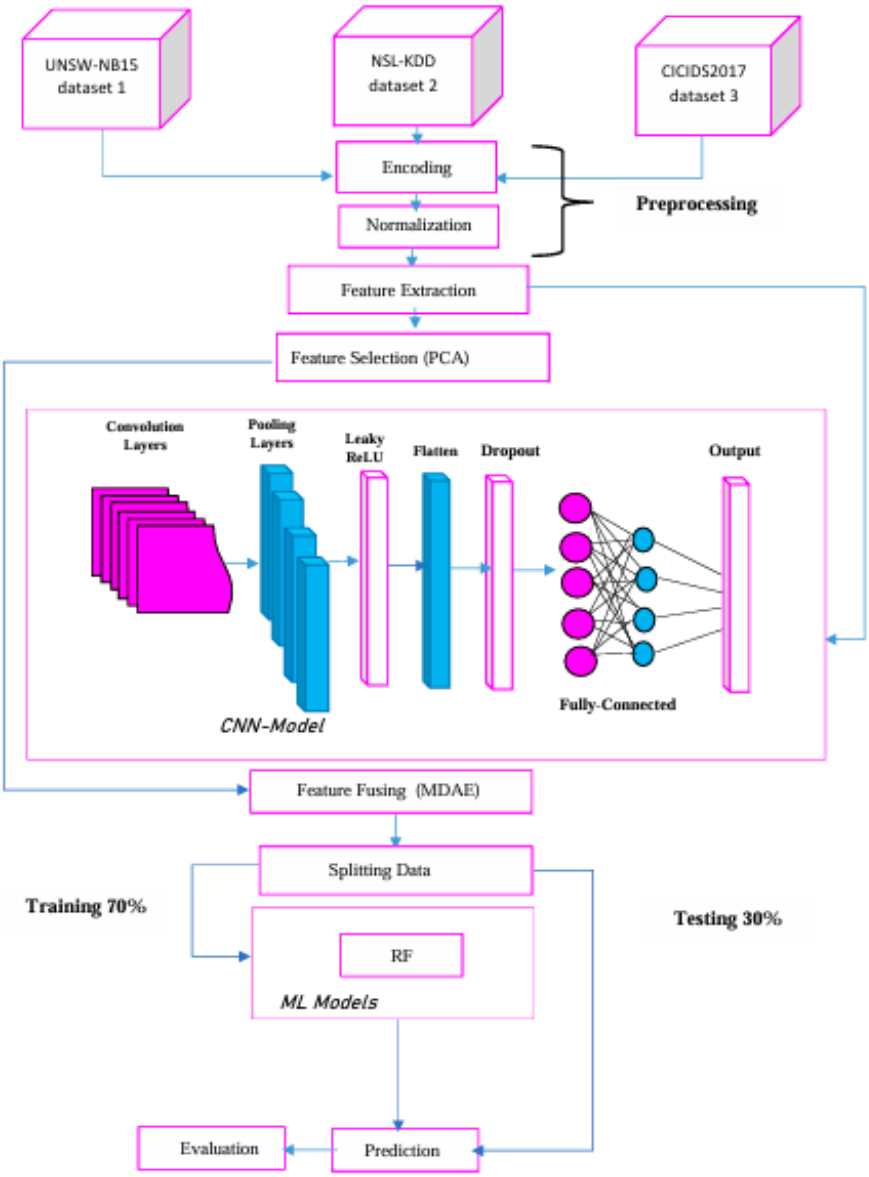

Fig.1 *The proposed methodology*

Dataset Description

Datasets are crucial for developing and assessing IDSs, as they verify the capacity for detecting and training malicious activities. Three of the most often utilized reference datasets in intrusion detection have been applied in this work:

• **NSL-KDD:** This dataset has been developed to solve problems, like uneven sample representation and data redundancy, enhancing the 1999 KDD Cup dataset. With 43 distinct features that characterize connection characteristics, protocol type, service, and attack type, the dataset is fit for assessing performance in semi-realistic environments. It also has over 125,973 samples.

• **UNSW-NB15:** Real-world network conditions were simulated in an advanced simulation environment. These are among the most varied and current datasets. This approach is ideal for evaluating models' ability to distinguish among various patterns. It offers 45 attributes, including information on protocols, ports, sessions, and network behaviours, and comprises 82,332 samples split into several categories of attack and usual activity. This article addresses a wide range of attack scenarios, from brute force attacks to denial-of-service (DoS and DDoS) attacks, as well as normal traffic.

• **CICIDS2017:** This dataset offers a comprehensive account of actual network traffic. Comprising 79 attributes and approximately 225,745 samples, it is a well-established standard for evaluating IDS performance in today's advanced settings.

Data Preprocessing

Three benchmark datasets, UNSW-NB15, NSL-KDD, and CICIDS2017, used in intrusion detection, are pre-processed using the suggested approach. In this phase, label encoding transforms class properties into numerical representations, and a normalizing technique is used to normalize numerical data within the range [0, 1]. This phase aims to ensure that the data meets the criteria of the deep model and accelerates the learning process.

Feature Extraction Using Convolutional Neural Networks (CNNs)

Features are extracted following preprocessing by feeding data from each dataset into a distinct CNN that is able to identify trends in network traffic. The dimensions of the input data are changed to satisfy CNN architectural criteria using pooling, convolution, and fully connected layers. This architecture captures the spatially accurate characteristics required to identify attacks and cyber threats. To extract features in an abstract manner, we applied the 1D CNN model separately to each dataset. The architecture is:

• Input shape: (number of examples, number of features, 1).
• Conv1D: 64 filters, kernel size=3, ReLU activation.
• MaxPooling1D: pool size=2.
• Flatten layer.
• Dense layer: 128 units, ReLU.
• Dropout: 0.5.
• Feature extraction layer: Dense (64), ReLU
• Output layer: Dense (number of input features), linear activation.
• Loss: MSE; Optimizer: Adam.

Feature Selection and Dimensionality Reduction

High dimensionality in the obtained features is addressed by a dimensionality reduction method, PCA, which also addresses redundancy. The PCA is performed on each dataset independently to lower the dimensionality of the CNN-extracted features while retaining the meaningful variance. We retained the top 20 components, which account for 95% of the cumulative variance. This approach reduces noise and enables the model to focus on the most critical features, thereby enhancing model performance.

Multi-Source Feature Fusion Using MDAE

Three reduced feature datasets are fused using an MDAE, creating a new, comprehensive dataset. These fusions enhance model accuracy and generalizability across various attacks. The MDAE architecture:

• Input: Input-dim.
• Encoder:
o Dense (64), ReLU.
o Dense (32), ReLU.
• Decoder:

o Dense (64), ReLU.
o Dense (Input-dim), Linear.
• Loss: Mean Squared Error.
• Optimizer: Adam.
• Epochs: 10.
• Batch size: 256.

Classification Using Random Forest (RF)

Following feature fusion, the main classification used is the RF model. One of the most powerful and reliable ML techniques, the RF aggregates the outputs of several decision trees by voting and generates more accurate results. This approach lessens the likelihood of overfitting and helps to effectively manage complex multimodal data. The classification is done using a Random Forest (RF) classifier:
• Number of estimators: 100.
• Max depth: None (nodes are expanded until pure).
• Criterion: Gini.

Experimental Setup

• Hardware: Intel Core i5-7200U, 16 GB RAM, Intel HD Graphics 620 (8267 MB).
• Software: Python 3.11, TensorFlow 2.13, Scikit-learn 1.3.0, NumPy, Pandas.

Results and Discussion

With high efficiency, the suggested intrusion detection model proved outstanding performance over various evaluation criteria. First, using CNNs to extract features from three well-known intrusion detection benchmark datasets (UNSW-NB15, NSL-KDD, and CICIDS2017), the suggested model precisely reflects hidden structures in the data. PCA was applied to solve the high dimensionality problem and eliminate redundancy, enhancing classification accuracy. Combining the three datasets using an MDAE produced a new dataset that nonlinearly reflects the structural variety in the data. After that, an RF model was trained on this set to enhance performance. With a classification accuracy rate of 99.9%, high precision, high recall, and an F1 score of 99.9%, the data provided in Table 1 highlight the outstanding predictive ability of the model. The model, built on the RF algorithm, demonstrated high performance in accurately and reliably classifying intrusion cases, effectively distinguishing between healthy cases (91901 true positives and 38251 true negatives) and attacks with a very limited number of errors (63 false positives and 0 false negatives). With significantly lower false negative and false positive rates, the confusion matrix shown in Figure 3 demonstrates the model's flexibility and reliability in distinguishing between "malicious" and "correct" actions. Built on multi-modal fusion methods, DL, and classification, the suggested model performs with higher accuracy and stability than conventional models, depending on single-source inputs or shallow classifiers. The results show that the RF model can effectively solve the problems presented by high-dimensionality and heterogeneity of network data distribution, employing nonlinear multi-source data fusion employing MDAE. This enables the design of more reliable and intelligent IDSs in challenging environments. Figure 2 shows the frequency graph of the new data. Our model uses three diverse datasets, simulating a wide range of attack scenarios. However, real-time generalization on live network streams remains future work. Deployment on streaming platforms, such as Apache Kafka, is recommended. Table 2 shows the assessment of the contribution

of each component of the proposed model to the overall performance. Table 3 presents a comparison of the proposed model with the latest methods from related studies.

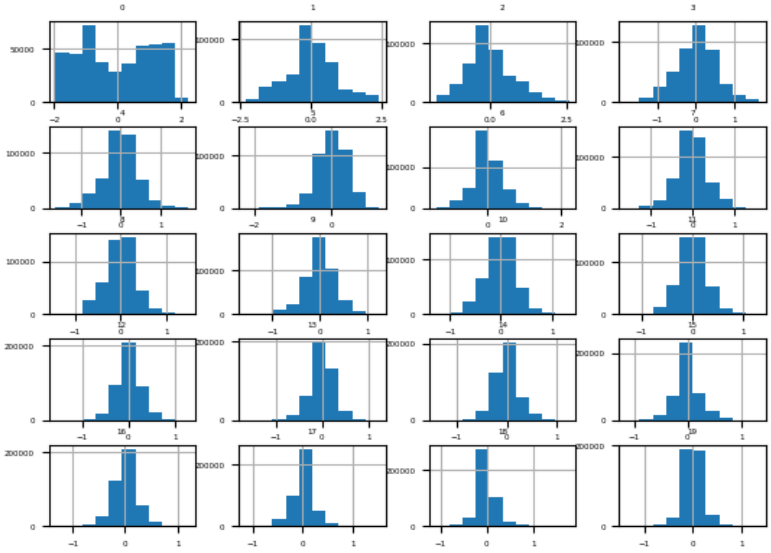

Fig.2 *Histogram Plot for the new dataset.*

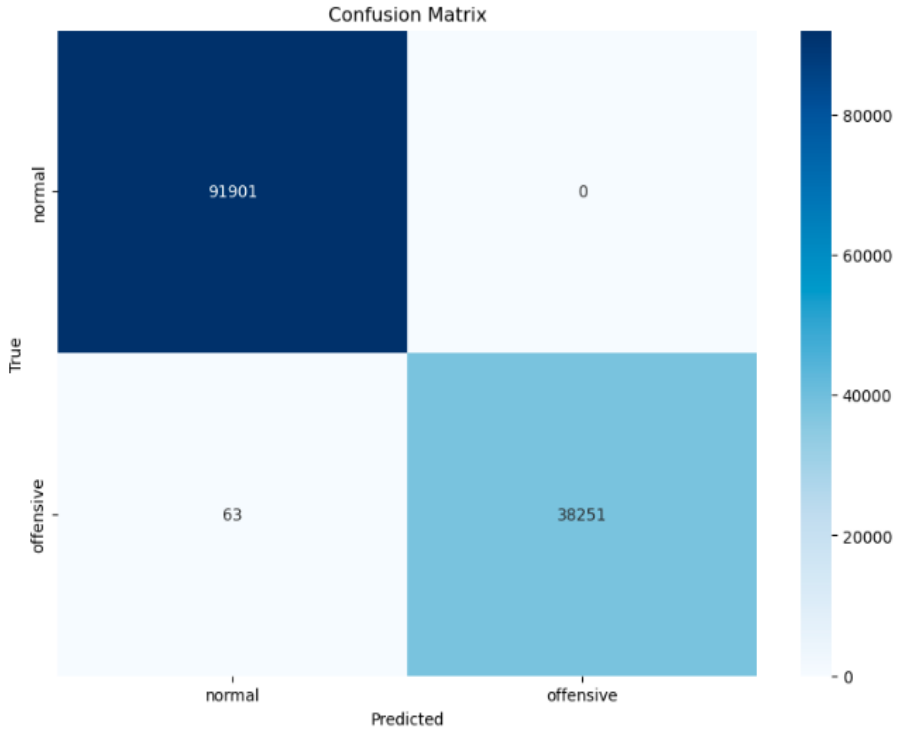

Fig.3 *Confusion Matrix.*

Table 1: Evaluation metrics.

Sequence	Metrics	Performance
1	Accuracy	99.9%
2	Precision	99.9%
3	Recall	99.9%
4	F1-score	99.9%

Table 2: To assess the contribution of each component of the proposed model.

Experimental Setup	Remarks
Full model (CNN+PCA+MDAE+RF)	High performance with all components.
Without PCA	Performance drops due to redundant features.
Without CNN	Significant degradation in feature quality.
MDAE+RF Only	Acceptable performance, but lower than full model.
RF on raw feature only	Low performance baseline.

Table 3: Comparison.

Reference	Model	Dataset
[19]	CNN	NSL-KDD, CSE-CIC-IDS2018.
[2]	OCNN-HMLSTM	NSL-KDD, ISCX-IDS, UNSW-NB15.
[20]	CNN-IDS	UNSW-NB15, Bot-IOT.
[24]	DCNN	ISCX-IDS2012, CICIDS2017, CICIDS2018.
This work	CNN+PCA+MDAE+RF	NSL-KDD, CICIDS2017, UNSW-NB15.

Conclusion

This paper offered a successful and comprehensive framework for network intrusion detection through combining DL and ML techniques with a multimodal method. Features from three typical datasets were extracted using CNNs under the suggested approach. After that, dimensionality was reduced using dimensionality reduction methods, such as PCA, thereby enhancing performance. The three datasets were combined to produce a new dataset using an MDAE. The three datasets were combined, and an RF classification model was trained using the resultant data. With an outstanding classification accuracy of 99.9% and remarkable performance measures, including F1 score and recall, evaluation findings showed the model's capacity to distinguish between malicious and benign actions in complex network environments. Unlike conventional single-source solutions, this paradigm claims adaptability with heterogeneous data and enhanced generalization ability. MDAE helps to create a robust model to understand several network traffic patterns by tackling the problems presented by several data sources. These findings show the possibility of using a multi-modal method based on DL to improve IDS performance. To create more resilient and responsive systems in the future, utilizing continuous learning approaches, immediate deployment of

models, and integrating more advanced architectures is recommended to address increasingly expanding and complex cyber threats.

Limitations and Future Work

• Real-time deployment and incremental learning were not implemented.
• Deep models require significant computational resources.
• Future directions include transformer-based fusion, lightweight CNNs, and deployment in cloud-native systems.

References

1. S. Mane and D. Rao, "Explaining network intrusion detection system using explainable AI framework," *arXiv Prepr. arXiv2103.07110*, 2021.
2. P. R. Kanna and P. Santhi, "Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features," *Knowledge-Based Syst.*, vol. 226, p. 107132, 2021.
3. A. T. Assy, Y. Mostafa, A. Abd El-khaleq, and M. Mashaly, "Anomaly-based intrusion detection system using one-dimensional convolutional neural network," *Procedia Comput. Sci.*, vol. 220, pp. 78–85, 2023.
4. M. Kumar and A. K. Singh, "Distributed intrusion detection system using blockchain and cloud computing infrastructure," in *2020 4th international conference on trends in electronics and informatics (ICOEI)(48184)*, IEEE, 2020, pp. 248–252.
5. L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Comput. Sci.*, vol. 185, pp. 239–247, 2021.
6. M. M. Hamood, M. L. Shuwandy, and R. A. F. Alsharida, "Enhancing Smartphone Authentication by Integrating Decision-Making Model with Touch Pressure, Finger Location Data, and Advanced Cybersecurity Techniques," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 4, p. 26, 2024.
7. T. P. Quinn *et al.*, "A primer on the use of machine learning to distil knowledge from data in biological psychiatry," *Mol. Psychiatry*, vol. 29, no. 2, pp. 387–401, 2024.
8. A. Halimaa and K. Sundarakantham, "Machine learning based intrusion detection system," in *2019 3rd International conference on trends in electronics and informatics (ICOEI)*, IEEE, 2019, pp. 916–920.
9. Q. Alasad, M. M. Hammood, and S. Alahmed, "Performance and Complexity Tradeoffs of Feature Selection on Intrusion Detection System-Based Neural Network Classification with High-Dimensional Dataset," in *International Conference on Emerging Technologies and Intelligent Systems*, Springer, 2022, pp. 533–542.
10. E. P. Cynthia *et al.*, "Convolutional Neural Network and Deep Learning Approach for Image Detection and Identification," in *Journal of Physics: Conference Series*, IOP Publishing, 2022, p. 12019.
11. L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A mean convolutional layer for intrusion detection system," *Secur. Commun. Networks*, vol. 2020, no. 1, p. 8891185, 2020.
12. I. Lauriola, A. Lavelli, and F. Aiolli, "An introduction to deep learning in natural language processing: Models, techniques, and tools," *Neurocomputing*, vol. 470, pp. 443–456, 2022.
13. M. Shakir, A. B. Abubakar, Y. Yousoff, M. Al-Emran, and M. Hammood, "Application of

confidence range algorithm in recognizing user behavior through EPSB in cloud computing," 2016.
14. H. Benmeziane, "Comparison of deep learning frameworks and compilers," *Master Comput. Sci. École Natl. Supérieure d'Informatique*, 2020.
15. R. Zebari, A. Abdulazeez, D. Zeebaree, D. Zebari, and J. Saeed, "A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 1, pp. 56–70, 2020.
16. H. He, X. Sun, H. He, G. Zhao, L. He, and J. Ren, "A novel multimodal-sequential approach based on multi-view features for network intrusion detection," *IEEE Access*, vol. 7, pp. 183207–183221, 2019.
17. A. A. Ojugo and R. E. Yoro, "Empirical solution for an optimized machine learning framework for anomaly-based network intrusion detection," *Technol. Rep. Kansai Univ.*, vol. 62, no. 08, pp. 6353–6364, 2020.
18. W. Jo, S. Kim, C. Lee, and T. Shon, "Packet preprocessing in CNN-based network intrusion detection system," *Electronics*, vol. 9, no. 7, p. 1151, 2020.
19. J. Yoo, B. Min, S. Kim, D. Shin, and D. Shin, "Study on network intrusion detection method using discrete pre-processing method and convolution neural network," *IEEE Access*, vol. 9, pp. 142348–142361, 2021.
20. M. Gamal, H. M. Abbas, N. Moustafa, E. Sitnikova, and R. A. Sadek, "Few-shot learning for discovering anomalous behaviors in edge networks," *Comput. Mater. Contin.*, vol. 69, no. 2, pp. 1823–1837, 2021.
21. J. Yin *et al.*, "Internet of things intrusion detection system based on convolutional neural network," *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 2119–2135, 2023.
22. Z. Wang and F. A. Ghaleb, "An attention-based convolutional neural network for intrusion detection model," *IEEE Access*, vol. 11, pp. 43116–43127, 2023.
23. O. Berjawi, A. El Attar, F. Chbib, R. Khatoun, and W. Fahs, "Cyberattacks detection through behavior analysis of internet traffic," *Procedia Comput. Sci.*, vol. 224, pp. 52–59, 2023.
24. V. Hnamte and J. Hussain, "Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach," *Telemat. Informatics Reports*, vol. 11, p. 100077, 2023.
25. M. Zakariah, S. A. AlQahtani, A. M. Alawwad, and A. A. Alotaibi, "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset.," *Comput. Mater. Contin.*, vol. 77, no. 3, 2023.
26. S. P. Jadhav, A. Srinivas, P. D. Raghunath, M. R. Prabhu, J. Suryawanshi, and A. Haldorai, "Deep learning approaches for multi-modal sensor data analysis and abnormality detection," *Meas. Sensors*, vol. 33, p. 101157, 2024.
27. L. Wang, M. Xia, H. Hu, J. Li, F. Hou, and G. Chen, "FusionNN: A Semantic Feature FusionModel Based onMultimodal forWeb Anomaly Detection.," *Comput. Mater. Contin.*, vol. 79, no. 2, 2024.
28. A. D. Vibhute and V. Nakum, "Deep learning-based network anomaly detection and classification in an imbalanced cloud environment," *Procedia Comput. Sci.*, vol. 232, pp. 1636–1645, 2024.
29. A. D. Vibhute, M. Khan, C. H. Patil, S. V Gaikwad, A. V Mane, and K. K. Patel, "Network anomaly detection and performance evaluation of Convolutional Neural Networks on UNSW-NB15 dataset," *Procedia Comput. Sci.*, vol. 235, pp. 2227–2236, 2024.

IRAQI Academic Scientific Journals
Samarra Journal of Pure and Applied Science
SJPAS
مجلة سامراء للعلوم البحتة والتطبيقية
www.sjpas.com
p ISSN: 2663-7405
e ISSN: 2789-6838

نظام ذكي لكشف التطفل باستخدام التعلم العميق والاندماج متعدد الوسائط مع تصنيف الغابات العشوائية

نهى فارس عبد المجيد [1]*، ميثم مصطفى حمود[2]

1- قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة تكريت، تكريت، العراق البحث مستل من رسالة ماجستير الباحث الاول

معلومات البحث:

تأريخ الاستلام: 2025/06/03
تاريخ التعديل: 2025/07/18
تأريخ القبــول: 2025/08/16
تاريخ الـنشر: 2026/04/10

الكلمات المفتاحية:

IDS، CNN، DL، ML، متعدد الوسائط، RF.

معلومات المؤلف

الايميل:-Nuha.F.abdEl
majeed4238@st.tu.edu.iq
الموبايل: 07705142324

الخلاصة:

ازداد الطلب المُلِحّ على أنظمة كشف التسلل (IDS) الفعّالة والذكية للتعامل مع هذه المشكلة، تماشيًا مع التعقيد والتنوع المتزايدين للهجمات الإلكترونية. باستخدام أساليب التعلم العميق (DL)، تهدف الدراسة المُقدَّمة إلى بناء إطار عمل مُتكامل يُعزِّز دقة كشف التسلل وقابلية تعميمه عبر مصادر بيانات مُتعدِّدة. في هذا العمل، استُخدمت ثلاث مجموعات بيانات معروفة، وهي UNSW-NB15 وNSL-KDD وCICIDS2017. يستخدم النهج المُقترَح الشبكات العصبية التلافيفية (CNNs) لاستخراج السمات العميقة من هذه المجموعات. يتم تقليل الأبعاد ويتم التخلص من السمات غير ذات الصلة باستخدام تحليل المُكوّن الرئيسي (PCA). يُستخرج من خلال دمج مجموعات البيانات الثلاث باستخدام مُرمِّز ذاتي عميق متعدد الوسائط (MDAE) مجموعة بيانات جديدة. يستخدم التصنيف النهائي تقنية الغابة العشوائية (RF)، مما يُصنِّف حركة مرور الشبكة بكفاءة ودقة باستخدام البيانات المُجمَّعة. بفضل الدقة العالية، ودرجة F1، ونسبة التذكر البالغة 99.9%، تُظهر نتائج التقييم دقةً ممتازةً للنموذج تبلغ 99.9%. تُظهر هذه النتائج مدى كفاءة دمج خوارزميات التصنيف الحديثة، واستخراج الميزات، وأساليب دمج البيانات متعددة الوسائط لإنشاء نموذج متطور لكشف التسلل، قادر على الدفاع بكفاءة وثبات ضد الهجمات الصعبة.