Detecting Identity Theft Attacks in Cloud Security based on Artificial Intelligence Techniques

Qusay Kanaan Kadhim[1], Shaymaa Taha Ahmed[1], Juliet Kadum[1], Ekhlas Muthanna Turki [1] and Ahmed Kanaan Kadhim[2]

[1]*Department of Computer Science, University of Diyala, 32001 Baqubah, Iraq*

[2]*Department of Electrical and Electronic Engineering, Istanbul Gelisim University, 34310 Avcılar Istanbul,Turkey*

dr.qusay.kanaan@uodiyala.edu.iq, shaimaaAhmed@uodiyala.edu.iq, julietkadum@uodiyala.edu.iq,Umhumam15@gmail.com, ahmed.kanaan.alzaidi@gmail.com

Keywords: Detecting Identity, Denoising AutoEncoder (DAE), Long Short-Term Memory (LSTM), Theft Attacks.

Abstract: Identity theft attacks are among the most critical security challenges in cloud computing environments, as they allow malicious actors to gain unauthorized access to sensitive data and cloud-based services. With the rapid expansion of cloud computing applications, the need for intelligent and proactive defense mechanisms has become increasingly vital. This study introduces an Artificial Intelligence (AI) framework designed to detect and mitigate identity theft attempts by leveraging the Denoising AutoEncoder (DAE) and Long Short-Term Memory (LSTM) algorithms. The DAE component efficiently removes noise and extracts essential features from input data, while the LSTM network captures temporal dependencies to enhance anomaly detection. The proposed model was evaluated using a conventional cloud infrastructure, achieving a high detection accuracy of 94.90% with a notably low false positive rate. These results highlight that integrating AI-driven models such as DAE and LSTM can substantially strengthen cloud computing security by enabling early detection and prevention of identity theft attacks.

1 INTRODUCTION

Cloud computing is a new approach that combines previous technologies to create a new model that allows users to access shared modifiable resources on demand over the Internet. The cloud has many advantages but it also has several disadvantages such as vulnerability to attacks dependence on network connectivity service downtime supplier monopoly and limited control [1]. From another perspective this data availability encourages cyber attackers to exploit unknown vulnerabilities and bypass the know signatures [2]. One of the promising network solutions is Intrusion Detection System (IDS) [3]. The IDSs are classified in different ways one such classification is based on the detection method. In this way of classification IDSs are broadly divided into two categories [4]. One is a signature-based or misuse detection method and the other is an anomaly-based detection method [5]. In the signature based method the data points are compared with the previously known signatures and if there is a match an alarm is generated in an anomaly based detection [6].

The method a pattern is created based on the normal traffic and if there is a deviation from that pattern it is considered as an abnormal transaction [7]. Both methods have their own pros and cons. The signature-based method is good for detecting know attacks [8]. IDS are crucial technologies for defending systems and networks against unauthorized access and malicious assaults [9]. An intrusion detection system relies on a database containing signatures of known attacks [10]. This database is used as a reference to identify new attacks that resemble previously detected and analyzed attacks. The intrusion detection system scans network traffic for suspicious or malicious activity that violates security policy and notifies the system administrator when such activity is detected [11]. These systems monitor network traffic to detect any suspicious activity and issue alerts when such activity is detected.

However, they can generate false alarms so network intrusion detection systems require the use of complex algorithms and techniques to ensure high accuracy and effectiveness in detecting cyberattacks and distinguishing between suspicious and malicious

activities. The use of artificial intelligence especially deep learning and machine learning technology is essential to provide an improved security system by analyzing security data [12].

Recent studies by academics and information security managers in governments and scientific companies indicate the possibility of implementing deep learning (DL) machine learning to detect attacks as DL provides its capabilities in many fields [13]. When identifying risks and threats traditional manual methods have limited performance and high latency [14]. Attacks can be detected faster and more effectively using machine learning techniques [15]. In specific because of their remarkable performance deep learning models have been essential in identifying attacks [16].

Identity theft assaults are one of the most serious security risks in cloud computing environments since they allow attackers unauthorized access to private information and services. As cloud computing services are utilized more frequently, there is a greater need for intelligent systems that can identify these assaults in their early stages and lessen their effects [17].

This research study contributes to identifying flaws related to identity theft and breach detection in general, and this study provides an AI-based framework. These findings demonstrate that the security of cloud computing systems can be significantly improved by incorporating artificial intelligence methodologies.

2 LITERATURE REVIEW

The CICIDS2017 data set served as the basis for the experiment [18]. The researchers in the study, which was released in reference, used two feature selection methods along with seven separate classifications, including recurrent, random decision tree, simple categorization, and others filtered classification, random data clustering, random association, random decision forest, and decision tree [19]. They came to the conclusion that the best results were achieved by using AI-based feature selection methods in conjunction with a random decision tree classifier as opposed to other feature combinations techniques for selection and algorithms for classification [20].

In [21] S. Choudhary and N. Kesswani studied a victim-end-based DoS identification using an Deep Neural Network (DNN). The back-propagation and feed-forward approaches were used in this study. The first step was data collection from network traffic the second step was feature elimination and the third step was classification. The datasets used in these experiments were NSL-KDD resulting in an overall accuracy of 90 % Precision 82.3 % DR 85.1 % and F1-score 75.3 %.

In [22] Mustapha Belouch et al uses Detrain and Detest for training and testing respectively to perform a Deep Learning (DL) is a modern over the NSL-KDD without distinguishing between different attack types using LSTM algorithm resulting in an overall accuracy 82 % Precision 92.4% DR 79.0% and F1-score 82.2%.

In [23] The performance of the deep forest model was compared with SVM, NB, RF and DNN algorithms on NSL-KDD datasets. Resulting in an overall accuracy of 91.21% a precision of 92.0% a DR of 88.3% and an F1 score of 93.7% with the SVM and DNN algorithms.

In[24] Sharmin Aktar Abdullah Yasin Nurauthors evaluation Metric comparison for NSL-KDD dataset to track detection using deep learning applications for LSTM and AE VAE Our Approach Basic DAE of the resulting in an overall accuracy. The Basic DAE got resulting in an overall accuracy of 96.8 % Precision 96.8 % DR 96.8 % and F1-score 96.8 % on NSL-KDD dataset.

In [25] Harini R.Maheswari N.Ganapathy et al Metrics Comparison using deep learning on NSL KDD Dataset using CNN + BiLSTM for minority attack categories to evaluate the system resulting in an overall accuracy of 83.58 % Precision 85.14 % DR 85.82 % and F1-score 84.49 %.

Developing more sophisticated and effective detection models has been a key focus of numerous research studies [26]. Using training datasets artificial intelligence and machine learning approaches have been applied to identify the underlying patterns that characterize attacks [27]. The most commonly used methods focus on rule based inductive classification and data clustering.

Detecting different types of network traffic attacks must be accurate and fast. This research examines the main factors influencing the classification of these attacks through a critical analysis and comparison of the methods and techniques used in previous studies. The main contribution of this research is to discuss the detection accuracy of previous methods, as well as to evaluate the performance of artificial intelligence techniques in processing features of cyber attacks.

3 METHODOLOGY

Identity theft attacks are among the most serious security threats in cloud computing environments as they allow attackers to gain unauthorized access to sensitive data and services. As cloud computing services are used more and more frequently, there is an increasing need for smart methods to identify these assaults early on and lessen their effects. To identify anomalies related to identity theft attempts, Figure 1 of this study presents an AI framework based on deep Denoising AutoEncoder (DAE) and Long Short-Term Memory (LSTM) algorithms. The suggested model, which uses DAE and LSTM to implement a standard cloud computing dataset, is tested for its ability to provide high detection accuracy and a low false positive rate. Prior research demonstrates that integrating AI technologies may successfully improve the security of cloud computing systems

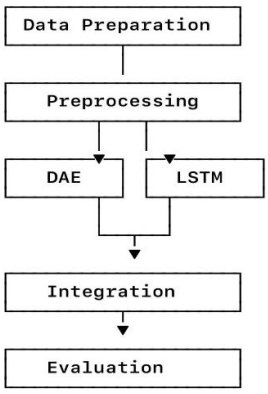

Figure 1: Suggested outline LSTM and DAE.

3.1 Dataset

The CICIDS2017 dataset, which is more diverse, is used in research papers to investigate both valid and illegal attempts to gain access to systems, as well as simulations of actual commercial settings. One of the most crucial aspects used to identify identity theft attacks in cloud computing environments is the CICIDS2017 dataset. Dataset link https://www.unb.ca/cic/datasets/ids-2017.html.

3.2 Preprocessing

In machine learning, data preparation is a necessary step prior to model development since it guarantees the correctness of the outcomes and aids in enhancing the model's overall performance. At this point, the data is cleaned, transformed, and prepared for training so that it can be used in models. Successfully completing this step is necessary in order to have a high-performing model that makes accurate predictions. Data are normalized by removing noise and missing values, then changing them to a set range, generally between 0 and 1. X' = (X - X_min) / (X_max - X_min) is the mathematical formula, where X_min is the smallest value in the dataset and X_max is the largest the maximum value in the dataset, which ensures that the features fall inside a specified range. Then divide it into training data that is divide the data into a training set and a testing set 80% for training and 20% for evaluation then a validation set and a test.

3.3 Denoising AutoEncoder

Delousing AutoEncoder (DAE) are a stochastic variant of traditional DAE which helps to reduce the risk of the network learning an identity function. DAE are a type of neural network used for feature selection and extraction also known as dimensionality reduction[28]. The more hidden layers in a DAE the more accurate the dimensionality reduction.

The input in this case is extremely particular; it only pertains to the attack packet data therefore the DAE does a fantastic job of classifying according to the attacks. The DAE will operate with the training dataset information and learn by applying back propagation from the training dataset results this is the decoder's phase as well as the necessary forward propagation to locate it has no significance. More than the phase from the encoder. Figure 2 provides a diagrammatic representation of how the DAE is implemented or works [29].

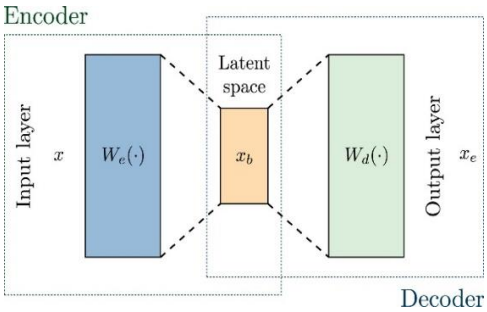

Figure 2: DAE architecture [30].

The hidden layers can be subjected to several encode and decode operations by the DAE (1) and (2) respectively contain the Eq. for the encode and decode procedures mentioned above.

Equation (1) provides the definition of the encoder function (e) assuming a Z-dimension vector.

$$Ei=e(Di,\theta e)\ Where\ Di^{-}\in Rn\ and Ei\in Rz. \quad (1)$$

Equation (2) also provides the decoder's parameterized function (d).

$$D^i=d(Ei,\theta d)\ Where\ Di^{\wedge}\in Rn\ and\ Ei\in Rz. \quad (2)$$

When encoded data are needed for a procedure the reverse propagation of the encoded data in order to decode them before the real data are needed. Equation (3) is offered to illustrate the same.

$$D^i=d(e(Di,\theta e),\theta d)=g(Di,\theta e). \quad (3)$$

The DAE uses the mean-square-error cost minimizer to propagate an encoded data backward. Equation (4) which provides the function describes the same.

$$Cost(D,D,\theta)=1/m\sum I(Di-g(Di,\theta)) \quad (4)$$

3.4 LSTM

Long Short-Term Memory (LSTM) is a deep learning algorithm known for its high accuracy and speed in classifying phishing emails. LSTM networks are an evolution of traditional recurrent neural networks differing from them in the structure of neurons[31]. The LSTM algorithm produces a two dimensional data separation plane which is used to identify message classes based on the input dataset. In phishing roads, the input data is processed according to specific criteria such as the presence or absence of a particular word or phrase and the LSTM system produces a value of 1 or 0 to determine whether the message is a phishing or not.LSTM technology is used to identify phishing emails improve performance and provide better classification results. Figure 3 illustrates how the LSTM Algorithm Network Architecture works as shown in the equation below.

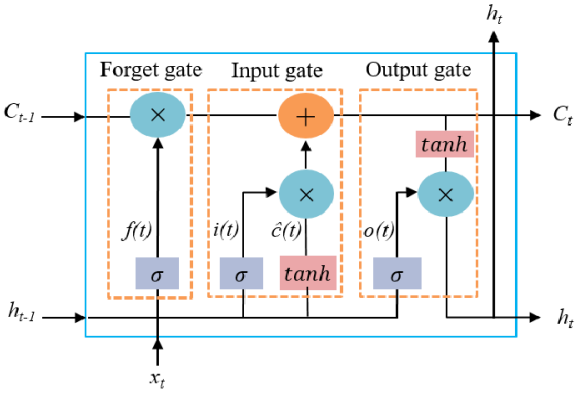

Figure 3: LSTM architecture[32].

3.5 Evaluation Metrics

The performance of the proposed fabric classification model was evaluated using a standard hold-out testing strategy [33]. After training, the dataset was divided into separate training and testing subsets to ensure an unbiased assessment of the model's generalization capability on unseen data.

To analyze classification performance in detail, a confusion matrix was constructed. This matrix provides a comprehensive view of correct and incorrect predictions across all fabric categories and serves as the basis for deriving quantitative performance metrics.

The evaluation was performed using widely adopted classification metrics, including accuracy, precision, and recall [34]. Accuracy represents the overall proportion of correctly classified samples among all predictions. Precision measures the reliability of positive predictions by indicating how many of the predicted samples for a given class are correctly classified. Recall reflects the model's ability to correctly identify all relevant samples of a given class.

In this study, these metrics are used to provide a balanced evaluation of model performance, particularly in distinguishing visually similar fabric types under varying illumination and texture conditions. The combination of confusion matrix analysis and class-wise performance metrics allows for a detailed assessment of both overall accuracy and per-class classification behavior.

4 RESULTS AND DISCUSSION

This paper presents results and a comparative analysis of artificial intelligence techniques for detecting denial-of-service attacks in cloud computing environments. The results of all applied methods are presented and the proposed approach is evaluated across different test scenarios focusing on the highest accuracy performance of the deep learning method as shown in Table 1

Based on the results in Table 1 we propose an AI framework that utilizes Long Short-Term Memory (LSTM) and Denoising AutoEncoder (DAE) algorithms to detect anomalies associated with identity theft attempts.

The results demonstrate that DAE and LSTM achieved a high detection accuracy of 94.90% with a low false positive rate.

Table 1: Comparative performance analysis results.

Methods	Accuracy %	Precision %	DR %	F1-score %
DNN	88.64	82.30	85.1	75.30
LSTM	90.62	92.40	89.4	82.20
SVM + DNN	91.21	90.80	88.3	90.70
CNN + BiLSTM	92.58	91.70	91.6	88.49
LSTM + DAE	94.90	92.20	91.8	93.4

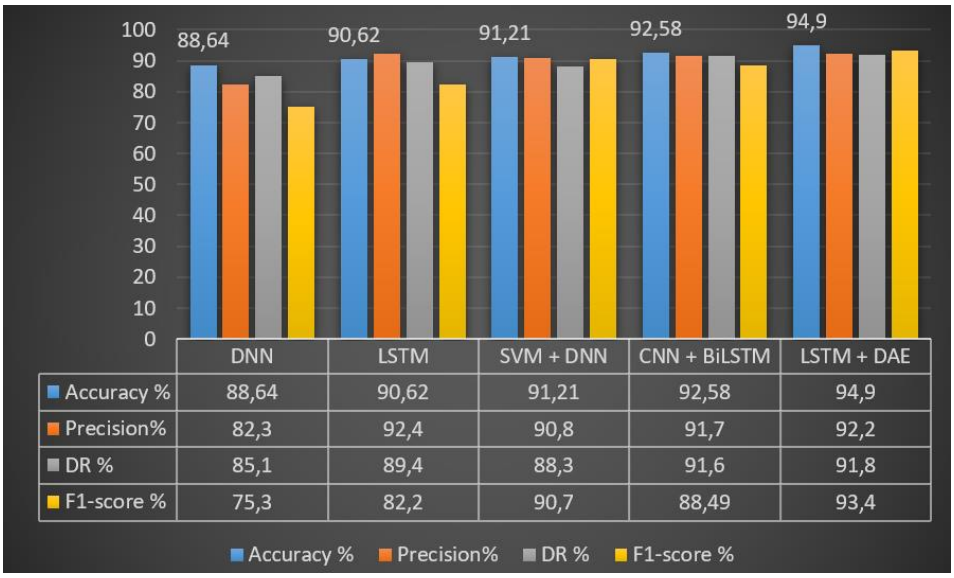

Figure 4: Results of the evaluation of using artificial intelligence technologies.

These findings suggest that integrating AI technologies can effectively enhance the security of cloud computing systems. In Figure 4 the proposed DAE and LSTM technologies are evaluated for detection rate and false positive rate using metrics such as accuracy detection rate and false positive rate to measure the implementation performance in a cloud environment.

Figure 4 illustrates a critical analysis and comparison of the methods and techniques (DNN, LSTM, SVM+DNN, CNN+BiLSTM, and LSTM+DAE), and discusses the detection accuracy of AI methods and evaluates the performance of AI techniques in detecting identity theft attacks in cloud computing. It provides an AI-based framework. These results show that cloud computing security can be greatly improved by integrating artificial intelligence methodologies.

5 CONCLUSIONS

The need for intelligent mechanisms to detect and mitigate attacks is growing. Integrating Artificial Intelligence (AI) techniques into security systems improves data security against tampering and theft. Through predictive analysis, behavioral recognition, and malicious activity detection, it leads to improved detection of identity theft attacks in cloud security and faster, more effective incident response. Implementing AI security standards is critical to reducing risks and preventing unauthorized access, manipulation, or other forms of cyberattacks.

In this research study, we utilized AI techniques (DNN, LSTM, SVM + DNN, CNN + BiLSTM, and LSTM + DAE). Based on the results of this study, which showed that DAE and LSTM achieved a high detection accuracy of 94.90% with a low false positive rate, we propose an AI framework based on LSTM and DAE. To detect abnormalities associated with identity theft attempts at a low false positive rate.

Frameworks that improve the detection of identity theft attacks in cloud computing using AI techniques effectively guide and enhance cloud computing security by reducing resource burden and false positives, thereby minimizing vulnerabilities to cyber threats.

REFERENCES

[1] Q. K. Kadhim, A. I. Altameemi, R. M. Abdulkader, and S. T. Ahmed, "Enhancement of Data Center Transmission Control Protocol Performance in Network Cloud Environments," Ingénierie des systèmes d'information, vol. 29, no. 3, pp. 1115-1123, Jun. 2024, doi: 10.18280/isi.290329.

[2] S. A. Alansary, S. M. Ayyad, F. M. Talaat, and M. M. Saafan, "Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning," Knowledge and Information Systems, vol. 8, no. 8, pp. 1-37, Aug. 2025, doi: 10.1007/s10115-025-02556-6.

[3] V. Z. Mohale and I. C. Obagbuwa, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity," Frontiers in Artificial Intelligence, vol. 8, pp. 1-10, Jan. 2025, doi: 10.3389/frai.2025.1526221.

[4] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computers Networking Security," Computers, vol. 14, no. 3, p. 87, Mar. 2025, doi: 10.3390/computers14030087.

[5] S. Ennaji, F. De Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," IEEE Access, vol. 13, pp. 148613-148645, 2024, doi: 10.1109/ACCESS.2025.3600984.

[6] W. Sus and P. Nawrocki, "Signature-based Adaptive Cloud Resource Usage Prediction Using Machine Learning and Anomaly Detection," Journal of Grid Computing, vol. 22, no. 2, pp. 1-15, Jun. 2024, doi: 10.1007/s10723-024-09764-4.

[7] A. I. Altameemi, S. J. Mohammed, Z. Q. Mohammed, Q. K. Kadhim, and S. T. Ahmed, "Enhanced SVM and RNN Classifier for Cyberattacks Detection in Underwater Wireless Sensor Networks," International Journal of Safety and Security Engineering, vol. 14, no. 5, pp. 1409-1417, Oct. 2024, doi: 10.18280/ijsse.140508.

[8] M. H. Nasir, J. Arshad, and M. M. Khan, "Collaborative device-level botnet detection for internet of things," Computers & Security, vol. 129, p. 103172, 2023, doi: 10.1016/j.cose.2023.103172.

[9] U. Ahmed et al., "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," Scientific Reports, vol. 15, no. 1, p. 1726, Jan. 2025, doi: 10.1038/s41598-025-85866-7.

[10] H. H. Saleh and S. T. Hasson, "Improving Communication Reliability in Vehicular Networks Using Diversity Techniques," Journal of Computational and Theoretical Nanoscience, vol. 16, no. 3, pp. 838-844, Mar. 2019, doi: 10.1166/jctn.2019.7963.

[11] E. Emirmahmutoğlu and Y. Atay, "A feature selection-driven machine learning framework for anomaly-based intrusion detection systems," Peer-to-Peer Networking and Applications, vol. 18, no. 3, pp. 1-28, May 2025, doi: 10.1007/s12083-025-01947-4.

[12] S. J. Abdu-al Kadhm, "Contactless Palmprint Recognition using Deep Learning Technology," Academic Science Journal, vol. 2, no. 1, pp. 361-370, Jan. 2024, doi: 10.24237/ASJ.02.01.678B.

[13] I. Mishkhal, N. Abdullah, H. H. Saleh, N. I. R. Ruhaiyem, and F. H. Hassan, "Facial Swap Detection Based on Deep Learning: Comprehensive Analysis and Evaluation," Iraqi Journal of Computer Science and Mathematics, vol. 6, no. 1, pp. 1-15, Feb. 2025, doi: 10.52866/2788-7421.1229.

[14] L. Algorithm, "The Detection of Fake Text News using a Dense-based 1D-CNN Deep Learning Algorithm," Academic Science Journal, vol. 2, no. 2, pp. 156-171, Apr. 2024, doi: 10.24237/ASJ.02.02.728B.

[15] T. Joseph Akinbolaji, "Advanced Integration of Artificial Intelligence and Machine Learning for Real-Time Threat Detection in Cloud Computing Environments," Iconic Research and Engineering Journals, vol. 6, no. 10, pp. 980-991, 2023.

[16] M. Alwan Hasson, "The Use of Convolution Neural Networks to Classify Viral Pneumonia and COVID-19 by Using Chest X-ray Images," Academic Science Journal, vol. 2, no. 1, pp. 291-304, Jan. 2024, doi: 10.24237/ASJ.02.01.706D.

[17] D. M. A. A. Afraji, J. Lloret, and L. Peñalver, "Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments," Cyber Security Applications, vol. 3, p. 100085, Dec. 2025, doi: 10.1016/j.csa.2025.100085.

[18] M. Sajid et al., "Enhancing intrusion detection: a hybrid machine and deep learning approach," Journal of Cloud Computing, vol. 13, no. 1, p. 123, Jul. 2024, doi: 10.1186/s13677-024-00685-x.

[19] D. Sudyana et al., "Improving Generalization of ML-Based IDS With Lifecycle-Based Dataset, Auto-Learning Features, and Deep Learning," IEEE Transactions on Machine Learning in Communications and Networking, vol. 2, pp. 645-662, 2024, doi: 10.1109/TMLCN.2024.3402158.

[20] I. Nazeeh, T. Hussain Hadi, Z. Qahtan Mohammed, S. Taha Ahmed, and Q. Kanaan Kadhim, "Optimizing blockchain technology using a data sharing model," Indonesian Journal of Electrical Engineering and Computer Science, vol. 29, no. 1, p. 431, 2023, doi: 10.11591/ijeecs.v29.i1.pp431-440.

[21] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," Procedia Computer Science, vol. 167, pp. 1561-1573, 2020, doi: 10.1016/j.procs.2020.03.367.

[22] M. Mustapha Belouch and Salah ElHadaj, "A Survey on Machine Learning based Intrusion Detection Systems Using Apache Spark," in 2021 5th High Performance Computing and Cluster Technologies Conference, New York, NY, USA: ACM, Jul. 2021, pp. 20-26, doi: 10.1145/3497737.3497740.

[23] R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique," Cybersecurity, vol. 5, no. 1, pp. 1-12, 2022, doi: 10.1186/s42400-021-00103-8.

[24] S. Aktar and A. Yasin Nur, “Towards DDoS attack detection using deep learning approach,” Computers & Security, vol. 129, pp. 1-16, 2023, doi: 10.1016/j.cose.2023.103251.

[25] R. Harini, N. Maheswari, S. Ganapathy, and M. Sivagami, “An effective technique for detecting minority attacks in NIDS using deep learning and sampling approach,” Alexandria Engineering Journal, vol. 78, pp. 469-482, 2023, doi: 10.1016/j.aej.2023.07.063.

[26] V. Kandasamy and A. A. Roseline, “Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks,” Scientific Reports, vol. 15, no. 1, p. 1697, Jan. 2025, doi: 10.1038/s41598-025-85547-5.

[27] S. Ankalaki, A. R. Atmakuri, M. Pallavi, G. S. Hukkeri, T. Jan, and G. R. Naik, “Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence,” IEEE Access, vol. 13, pp. 44662-44706, 2025, doi: 10.1109/ACCESS.2025.3547433.

[28] L. K. G. Danquah, S. Y. Appiah, V. A. Mantey, I. Danlard, and E. K. Akowuah, “Computationally Efficient Deep Federated Learning with Optimized Feature Selection for IoT Botnet Attack Detection,” Intelligent Systems with Applications, vol. 25, p. 200462, Mar. 2025, doi: 10.1016/j.iswa.2024.200462.

[29] W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, “Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine,” IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1634-1646, 2022, doi: 10.1109/TCC.2020.3001017.

[30] G.-F. Angelis, C. Timplalexis, S. Krinidis, D. Ioannidis, and D. Tzovaras, “NILM applications: Literature review of learning approaches, recent developments and challenges,” Energy and Buildings, vol. 261, p. 111951, Apr. 2022, doi: 10.1016/j.enbuild.2022.111951.

[31] M. Hosseinzadeh et al., “Improving phishing email detection performance through deep learning with adaptive optimization,” Scientific Reports, vol. 15, no. 1, p. 36724, Oct. 2025, doi: 10.1038/s41598-025-20668-5.

[32] S. Mohsen, A. Elkaseer, and S. G. Scholz, “Industry 4.0-Oriented Deep Learning Models for Human Activity Recognition,” IEEE Access, vol. 9, pp. 150508-150521, 2021, doi: 10.1109/ACCESS.2021.3125733.

[33] H. Wu, X. Li, and Y. Deng, “Deep learning-driven wireless communication for edge-cloud computing: opportunities and challenges,” Journal of Cloud Computing: Advances, Systems and Applications, 2020.

[34] T. S. Oyinloye, M. O. Arowolo, and R. Prasad, “Enhancing cyber threat detection with an improved artificial neural network model,” Data Science and Management, vol. 8, no. 1, pp. 107-115, Mar. 2025, doi: 10.1016/j.dsm.2024.05.002.